DEVELOPMENT OF PROTOTYPE GUIDELINES FOR RISK MANAGEMENT AGAINST TERROR ATTACK IN THE TOURISM INDUSTRY: A DELPHI STUDY

A Dissertation

by

CLIFFORD KEITH SMITH

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2006

Major Subject: Educational Human Resource Development

DEVELOPMENT OF PROTOTYPE GUIDELINES FOR RISK MANAGEMENT AGAINST TERROR ATTACK IN THE TOURISM INDUSTRY: A DELPHI STUDY

A Dissertation

by

CLIFFORD KEITH SMITH

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Walter F. Stenning
Committee Members,	Kenneth E. Paprock
	Stephen L. Stark
	James B. Kracht
Head of Department	Jim Scheurich

May 2006

Major Subject: Educational Human Resource Development

ABSTRACT

Development of Prototype Guidelines for Risk Management Against Terror Attack in the Tourism Industry: A Delphi Study. (May 2006)

Clifford Keith Smith, B.S., Texas A&M University; M.S., Texas A&M University

Chair of Advisory Committee: Dr. Walter F. Stenning

The purpose of the study was to gather strategies and factors from tourism security professionals from which terrorism risk management policies can be developed. This study utilized the Delphi method in order to provide structure for the group process. Twelve tourism security experts made up the panel completing three rounds of questionnaires via the email based Delphi technique.

This research identified fifty-four strategies to reduce the propensity of terror attack at a tourism venue. Those strategies were divided into four levels of priority based on criticality and feasibility. The fifty-four strategies were grouped into nine subordinate categories. The subordinate categories were related to Training, Communications/ Liaison, Planning/ Assessment, Background Checks, ID Badges/ Secure Entrance, Specialty Security Units, Architectural Design, Media Cooperation, and Technology Based strategies. Alongside the strategies are a collection of comments by the experts regarding strengths, weaknesses, and any barriers to implementation pertaining to the individual strategy. Tourism risk managers, security personnel, and insurance underwriters can all use the results in reducing the opportunity for a terrorist attack at a tourism venue.

Major research findings from this study included:

1. The strategy receiving the highest criticality ranking over all other strategies involves training first responders on their role in circumventing the success of terrorists.

2. The subordinate category Communication/ Liaison contains the largest number of strategies indicating the significance of this category among experts.

3. The subordinate category of Specialty Security Units contains the second highest number of strategies indicating the importance of the topic among experts.

4. All of the technology based strategies fell into the lowest priority level.

Based on the findings of this study, researcher recommendations include:

1. The guidelines developed in this study should be used by operators of tourism venues to make the best use of limited resources.

2. National or international conferences should be established to further discuss these issues.

3. A greater number of communications mediums should be established to facilitate the exchange of ideas and experiences between affected professionals.

4. Insurance providers should use this information to establish validated guidelines so that, if prospective clients adhered to the recommendations, a reduction in premiums could be offered.

5. Other entities may benefit from this study, such as public school systems, the energy production industry, hospital systems, and pipeline systems.

ACKNOWLEDGMENTS

This work is dedicated to my father, who, after over thirty-six years of dedication to law enforcement, is still actively serving. From the top to the bottom, people owe a debt of gratitude to him and others like him who sacrifice so much to serve our country. I would also like to thank my mother who has tolerated the sacrifices that go along with the dangerous professions the men in her life have chosen and for always being there along the way. Thanks Mom and Dad for supporting my desire to complete this work.

To my committee; thank you for your guidance and recommendations. To Dr. Stenning, thank you for your friendship over the last twenty years, your guidance, and encouragement throughout the entire process. To Dr. Kracht, thank you for your encouragement and sense of direction in setting up this study. And to Dr. Stark, please accept my deep appreciation for you stepping in at a critical time and providing so much valuable insight in the final stages.

I would also like to express a debt of gratitude to the experts who took time out of their busy schedules to participate in this study. I could not have completed this work without them.

And finally, thanks to Dr. Peter Tarlow for helping me to keep a positive outlook throughout this process.

TABLE OF CONTENTS

CHAPTER Page

LIST OF TABLES

CHAPTER I

INTRODUCTION

Prior to September 11, 2001, the World Tourism Organization estimated the industry generated $456 billion on an annual basis worldwide, not including travel expenses (Tarlow, 2001b). Crimes against tourists, whether terrorist attacks or crimes of opportunity, have received international attention causing the tourism industry to reallocate diminishing resources toward building an image of safe travel (Muehsam, 1996).

In April of 2003, United States Special Forces captured fugitive terrorist Abu Abbas, who masterminded the 1985 hijacking of the Italian cruise ship Achille Lauro, once again reminding the world of attacks on tourists. A group called the Palestine Liberation Front, who held 410 passengers for two days, conducted the hijacking. During the incident, a disabled American passenger named Leon Klinghoffer was shot and thrown overboard ("U.S. troops capture", 2003).

In 1997, a terrorist group called The Jimat attacked a group of tourists at the Luxor in Egypt. The tourists who were murdered represented such countries as Japan, France, Switzerland, Germany and Great Britain. In all, there were sixty-eight tourists killed, proving once again that no nationality is safe from terrorist attack (Online Newshour, 1997). Following the attack, noted Egyptian political analyst and former information minister in the Egyptian Foreign Service, Mohammad Wahby, stated, "They target

---

The style and format followed will be that of the *American Educational Research Journal.*

tourists because this is the way which they think they can hit the government very, very hard. Tourism in Egypt is one of the biggest sources of revenues, and by depriving Egypt of this, they shake the very economic foundation of Egypt" (Online Newshour, 1997, p.2).

In October 2002, the bombing of a Bali nightclub killed 202 people, mostly foreign tourists, in the worst terrorist attack since the September 11, 2001 attacks in New York and Washington. The group responsible was the al Qaeda-linked terror group Jemaah Islamiyah ("Bali bomb plotter, 2003). In the aftermath, Bali's economy has lost hundreds of millions of dollars in tourist revenue ("Bali bomb lawyers", 2003).

Since tourists are free to choose their destination, a tourism location that becomes associated with terrorism can face a serious economic crisis. Therefore, in order to protect their image, tourist destinations should include crisis management as a part of the overall marketing/ management strategy (Sonmez, 1999).

Each segment of the tourism industry has its own individual and unique security concerns, but there may be areas of concern that are common among the various tourism sectors. This study will make an effort to identify commonalities in order to create a base from which to address terrorism risk management for the tourism industry.

Statement of the Problem

There is no set of guidelines to which the tourism industry can refer that would assist in the reduction of propensity for risk and loss due to terrorist attacks. A considerable foundation of knowledge has been produced in the literature regarding risk management; however, little is available specific to terrorism risk management in the tourism industry. The majority of research information on terrorism risk management has been developed

from personal contact with those individuals who are considered professionals within the tourism security field from a national as well as an international perspective. Those in the tourism industry, especially those countries vulnerable to politically motivated violence and those whose economic stability depends on tourism, need some guidance in order to reduce the risks involved with the tourism industry. This auspicious task begs for cooperation from a variety of professionals in order to develop practical guidelines for terrorism risk management professionals.

Purpose of the Study

The purpose of the study is to gather strategies and factors from tourism security professionals in order to formulate guidelines from which terrorism risk management policies can be developed. The researcher will attempt to correlate views and opinions regarding terrorism risk management and to allow respondents to react to and examine opposing viewpoints. The study shall put forth all possible options for consideration by individual, corporate, and agency policy makers. To provide further detail, an estimate of impact and consequences of any particular option as well as examination of the acceptability of any particular option shall be sought. The purpose of this study is NOT to make decisions for policy makers, but rather, to provide all available options presented by an informed group for consideration by policy makers.

Limitations and Assumptions

Risk management in general deals with topics ranging from financial risk management to accident prevention. The scope of this research shall encompass those areas of concern that may reduce the opportunity for or provide deterrence to a terror attack.

The major assumption involved with this study is the continuance of terrorism and its effects on travel and tourism. Daily updates from the U.S. Department of Homeland Security on the level of threat directed at United States and its interests seem to indicate that this.

Subject areas of risk management to be studied include, but are not limited to, risk assessment, emergency planning, response, and recovery. Additional ancillary matters would include relationships between the private sector and the public safety entities, Crime Prevention Through Environmental Design (CPTED), use of tabletop exercises for evaluation purposes, and hiring practices in the private sector including background checks.

There are several preempted segments of the Tourism Industry, which by the nature of their particular service, already have security models in place. Those would be the airline industry, the rail transport industry, and the cruise line industry. Also, governmental public safety entities are preempted because they are supposed to be in the business of risk management to the extent that they are trained in critical incident management and responsible for the preplanning of events within their perspective jurisdictions. The research plan for this study shall not consider the aforementioned as end users.

The end users of this research model shall be those in the Tourism Industry that operate within confined facilities such as, sporting arenas, convention halls, and theme parks. It is important in this work to create a list or "breakdown" of the major segments within the tourism industry that are affected by security threats or that can benefit from the research. A quick look provides the following list of potential end users:

1. Hotel/ Motel Industries
2. Transcontinental Busing Industry
3. Private Security Forces
4. Theme Parks and Major Attraction Parks
5. Sporting Event Hosts
6. Travel Agencies
7. Conference Centers

Research Questions

1. What are the needs of the Tourism Industry to reduce the risk of terrorist attack?
2. What are the solutions to the stated needs?
3. What are the barriers to the stated solutions?
4. What are the prototype guidelines to apply the solutions to the stated needs?

Definition of Terms

The following operational definitions will be utilized throughout the course of this research.

A background check is a process in which the specifics of an individual's past are revealed for the purposes of employment, obtaining access to classified information, or access to restricted areas.

CBRNE is the acronym for chemical, biological, radiological/ nuclear, explosive.

CPTED is the acronym Crime Prevention Through Environmental Design (Tarlow, 2002).

Contemporary Threat Management or CTM postulates that there is a connection between a specific set of behaviors in which the perpetrator engages prior to the violent act directed at the victim (Calhoun & Weston, 2003).

DHS stands for the United States Department of Homeland Security created after the attacks of 911.

DOI stands for the United States Department of Interior.

Tourism Crisis is any occurrence which can threaten the normal operation and conduct of tourism related businesses; damage a tourist destination's overall reputation for safety, attractiveness, and comfort by negatively affecting visitors' perceptions of that destination; and, in turn, cause a downturn in the local travel and tourism economy, and interrupt the continuity of business operations for the local travel and tourism industry, by the reduction in tourist arrivals and expenditures (Sonmez, 1997).

Risk Assessment is the systematic examination of hazards and the potential for the risks arising to cause harm (Glendon, 1995).

Risk Management is the technique of applying known methods of dealing with the problem of risk in a more effective and more ordered form and to devise new or improved methods of minimizing loss (Crockford, 1980).

Terrorism is the calculated employment or the threat of violence by individuals, sub-national groups, and state actors to attain political, social, and economic objectives in the violation of law (Alexander, 2002).

WTTC is the World Travel and Tourism Council; an international organization of travel industry executives promoting travel and tourism worldwide.

CHAPTER II

REVIEW OF THE LITERATURE

Defining Terrorism

"Terrorism is often defined as indiscriminate destruction of property and life for the purposes of furthering a political agenda" (Tarlow, 2002, p. 133). Benjamin Netanyahu, former Prime Minster of Israel, describes terrorism as "the deliberate and systematic assault on civilians to inspire fear for political ends" (2001, p. 8). He further expands his definition by broadening the meaning of "political ends" to include ideological or religious motives. The essence of terrorism is the attack of the innocent who are in no way involved in legitimate conflict. The farther the victim is from the cause of the terrorists, then the greater the amount of terror inflicted (Netanyahu, 2001). Meltzer describes terrorism as a policy of intimidation. In other words, it is the "exploitation of a state of intense fear, caused by the systematic use of violent means by a party of group, to get into power or to maintain power" (Meltzer, 1983, p. 6).

More important than finding a definition that encompasses all aspects of terrorism is the understanding of the phenomenon. Groups that are in some varying degree supported by nation-states and inspired by religious, nationalistic, or political zealotry will use any means to accomplish their goals, including the use of suicide and mass murder as a weapon. Their objective is to attract attention to their cause and to terrorize their enemies into submission (Dershowitz, 2002).

Terrorism vs. Criminal Activity

Terrorists are willing to give their lives in pursuit of media attention. Criminals, unlike terrorists, wish to avoid attention. Rather, they seek profit and see their activity at

tourism events as work. Terrorists seek media attention as a tool to induce political chaos. Therefore, any tourist attraction is a potential target for terrorists. This trend differentiates criminal activity and terrorism as two different antisocial behaviors. Table 1 relates the differences between criminal activity and terrorism. Risk managers in the tourism industry must understand the differences as they now face new challenges in dealing with the possibility of terror attacks (Tarlow, 2002).

Table 1
Major Differences Between Event Crime and Terrorism

	Crime	**Terrorism**
Goal	Usually economic or social gain	To gain publicity and sometimes sympathy for a cause
Usual type of victim	Person may be known to the perpetrator or selected because he or she may yield economic gain	Killing is random and appears to be more in line with a stochastic model; numbers may or may not be important
Defenses in use	Often reactive, reports taken	Some proactive devices such as radar detectors
Political ideology	Usually none	Robin Hood model, that is to say, the terrorist sees himself in a positive light
Publicity	Usually local and rarely makes the international news	Almost always is broadcast around the world
Most common forms in events industry are:	Crimes of distraction Robbery Sexual Assault	Domestic terrorism International terrorism Bombings Potential for biochemical attack

Table 1 (continued)

	Crime	**Terrorism**
Statistical accuracy	Often very low; in many cases, the travel and tourism industry does everything possible to hide the information	Almost impossible to hide; numbers are reported with great accuracy and repeated often
Length of negative effects on the local events industry	In most cases, it is short term	In most cases, it is long term, unless replaced by new positive image
Recovery strategies	▪ New marketing plans, assumes short-term memory of traveling public ▪ Probability ideals: "odds are it will not happen to you" ▪ Hide information as best as one can	▪ Showing of compassion ▪ Need to admit the situation and demonstrate control ▪ Higher levels of observed security ▪ Highly trained (in tourism, terrorism, and customer service) security personnel

Trends in Terrorism

In the late 1980's, terrorism had become somewhat subdued both internationally and in Western countries. Terrorism has now returned in new forms and with great ferocity. The new *modus operandi* has been demonstrated by the use of chemicals to attack in the heart of the Japanese. The bombing of subways began in Paris after nearly a decade of silenced terrorist activity. Rather than hostage taking, terrorists are resorting to bombing their target. In the 1980's, the punishment and sanctions handed out to hostage takers and their supporters deterred their overt acts and now terrorists attempt to avoid punishment by living deep and undetected within a society (Netanyahu, 2001).

In his comparative study of counter terrorism, Alexander states:

> There is an apparent trend toward more lethal and massive terrorist attacks. Modern terrorists are increasingly motivated by hatred, revenge, and religious and

> cult fanaticism. They are less constrained by the rational political calculus that has influenced most terrorists in the past and that limited mass killing. Above all, U.S. officials fear that terrorists with these inclinations, both domestic and international, may acquire and use increasingly available materials of mass destruction - biological, chemical, and radiological - to carry out unprecedented mass-casualty terrorism (2001, p.26).

From a historical perspective, terrorism started as a retail venture. Assassinations of individuals and ambushes or bombings on a small scale are examples. Moving into the modern era, terrorism is now planned on the wholesale scale. Now, weapons of mass destruction provide choices to terrorists so that large-scale damage is a real threat and can be used to strike fear and seek attention. Terrorists can now use small personnel numbers to achieve huge results, as evidenced by the attacks of September 11, 2001 (Alexander, 2001).

The intense media coverage of terror attacks gives the impression that terrorism is a successful method to achieve the goals of the terrorist. Rarely are the failures of the terrorist reported in the media; only the successful, horrific events receive recognition. Also, the international community has shown a weakness to condemn terrorists. As a result, aggrieved groups have found that terrorism is an attractive method to affect change (Alexander, 2001).

The Madrid, Spain bombing provides an example of such strategies. The Popular Party of Spain has been a steadfast supporter of President Bush's foreign policy. The bombing of the subway system just days before Spain's general election lead to a surprise victory for the Socialist Party, which in turn denounced President Bush's policies and

removed their troops from Iraq. The weakening of the Spanish government against terrorism has sent the message that terrorist attack is now a viable strategy in which to influence elections, thus making terrorism an effective form of policy. The Spanish population sent a message by changing support for the other party, thus giving credence to terrorism as a successful strategy (Marquardt, 2003).

In 1994, the Office of Special Operations and Low-Intensity Conflict conducted a study on the future of terrorism. Almost ninety-five percent of the projections from the study have been correct. Those projections included the rise in terrorism by religious fanatics, a bombing in mid-America by domestic terrorists, an attack on the World Trade Center by Muslims, and the possibility of a hijacked plane used to target the Pentagon or White House. The study also predicts that New York, Washington, and Las Vegas will be the three major targets of terrorists. Because of the trends, the hospitality industry will be one of the hardest hit and should prepare itself against such attacks (Goss, 2003).

A federal commission headed by formers Senators Gary Hart and Warren B. Rudman came to these conclusions about terrorism in September 1999:

- The most serious threat to our security may consist of unannounced attacks on American cities by terrorist groups using germ warfare.
- Another threat may be a well-planned cyber-attack on the East Coast's air traffic control system as some 200 commercial aircraft are trying to land safely in a morning's rain and fog.
- U.S. forces will be increasingly involved in humanitarian missions in trouble spots around the world, fueling resentment toward us.

- In one of its grimmest predictions, the report said that, “Americans will likely die on American soil, possible in large numbers (“National security”, 2005).

We can no longer ignore the fact that terrorists are able to attack on a large scale within the borders of the United States. They have demonstrated their ability to become more sophisticated in terms of capability and synchronization. Terrorists study the weaknesses of the physical protection of our establishments so as to impart the greatest impact of an attack (U.S. Department of Homeland Security, 2003).

Tourism as a Target

With the trends in terrorism to increase both the number and size of attacks, there is an obvious connection between tourism and terrorism. Tarlow provides some reasons for the interaction between terrorism and tourist events:

- Events are often close to major transportation centers.
- Events are big business.
- Events impact other industries such as restaurants, hotels, and entertainment.
- Events often draw media coverage.
- Events require tranquility or places where business can be conducted in a peaceful manner.
- Events must deal with people who have no history; thus, risk managers often do not have databases on delegates or attendees.
- Events are based on a constant flow of guests; thus, it is hard to know who is and who is not a terrorist.
- Events are the point where business and relaxation converge, and therefore guests often let down their guard (Tarlow, 2002, p. 135).

Because the tourism industry is worth billions and receives vast media attention, it should consider itself a high profile target for terrorism. If the large amount of money involved is not enough to realize being a target, then consider these political reasons:

Tourism is attacked by terrorists for a number of reasons: firstly because it is seen to be symbolic of capitalism; secondly, tourists represent western oppressive regimes; and thirdly, by attacking state-sponsored tourism, terrorism is seen as a way to influence political behavior (Gold, 2001).

The El'Gama fundamentalist group was motivated by these very same views when they attacked the Luxor in Egypt in 1997 killing fifty-eight tourists and brining Egyptian tourism to a halt (Gold, 2001). When tourists are specified as the target of an attack, there are two different reasons. The terrorists see the tourist as the symbol of the sending country or as part of the economic system of the host country. In the first case, as representatives of another country, it is much easier to distinguish the threatened group of people. In the latter case, it is much more difficult to identify potential victims as tourists, foreign or domestic (Glaesser, 2003).

Terrorism almost certainly carries a political message. Publicity is the goal in order to get that political message out. The higher the profile of an event, the more media attention it will receive. Tourism being a high profile industry must recognize itself as a target for terrorism (Tarlow, 2002).

The Economics of Security

The connection between tourism's money-making ability and the concept of security are undeniable. The perceptions tourists have of a travel location's management of safety and security strongly affect their behavior and decisions about destinations. Furthermore, concerns about travel safety in general have shown that the tourism industry is vulnerable to changes in the global security environment. When a security concern arises, a ripple effect can occur. If a location is perceived as unsafe, that perception can spread to an entire region or even the entire tourism system (Hall, 2003).

"Between September 11, 2001 and December 31, 2002 estimated losses in tourism revenue for U.S. cities and metropolitan areas totaled $12.5 billion" (Hall, 2003, p. 41). "Not since the Gulf War has there been such a downturn in the travel and tourism market as has been caused by the terrorist attack on September 11" (Hall, 2003, p. 83)

History shows the reaction of tourists to terrorist activity. Of the 28 million Americans who traveled abroad in 1985, 162 were killed or injured during terrorist activity. That is a probability of less than .00057% of becoming a terrorist's victim. Despite this low probability, in 1986 two-million Americans changed their international travel plans due to the previous year's terrorist activity.

A 1986 Gallop Poll revealed that 79% of Americans said they would decline foreign travel due to terrorism. The World Tourism Organization posits that in 1985, there was a loss of $105 billion of US currency on an international level due to terrorism. During the Gulf War in 1991, the U.S. Department of State recorded 275 terrorist incidents, which influenced international travel flows. Throughout the 1990's, countries across the globe experienced economic loss due to terrorism (Sonmez, 1999). The 2001 attacks on the

World Trade Center and the Pentagon are yet another reminder that political conflict and terrorism will endure.

More current information shows this trend to continue. A Harris poll conducted in April of 2003 among over two thousand adults reveals millions of people have decided to avoid traveling, fly less, and spend less time away from home due to terrorism. Fifty-six percent stated that travel risks for Americans outside the United States are worse than before the attacks of 9/11. Seventeen percent (which would equate to thirty-five million people) said their vacation plans were affected by the Iraq war and terrorism. Twelve percent decided to do less flying within the United States. Ten percent decided to stay home more. Six percent changed their vacation destination. And seven percent decided not to travel at all (Taylor, 2003).

The impact on the travel and tourism industries has been severe. The damage to the air industry has been greater than to any other sector and remains vulnerable. The implementation of security measures will be costly, yet unavoidable in order to restore tourists' confidence levels (Safe Democracy Foundation, 2005). Tourists are willing to accept a certain level of risk when making travel decisions. The amount of risk is greatly influence by the "credibility of the affected organization" (Glaesser, 2003, p. 56). Therefore, methods or strategies to deal with the relationship between tourism and terrorism are essential for the protection of life and economic prosperity for those who depend on the tourism industry.

In May of 1998, the 7th Annual Las Vegas Tourism Security Conference was held during which several themes emerged.

- Tourism protection requires joint partnerships. The partnerships

include all aspects of the security and safety industries, government, hotel managers, tourism agencies and offices;

- Tourism crime is an expense that the tourism industry can ill afford;
- There is a need for greater applied research into all aspects of crimes against tourists;
- Tourism must come to understand that it risks its industry viability if it flees from the problems of safety;
- Tourism safety cannot be handled solely on a local basis, it must be confronted on a national and international level;
- The need for security professionals and academics to network together and to exchange ideas on a continual basis (Tarlow, 2000, p. 2).

The May 2000 conference yielded similar themes showing a trend that is continuing. At the conference Dr. Peter Tarlow (2001a) stated, "As tourism continues to grow, it is essential that the industry work hard to create a safe and secure environment in which safety and security issues are examined thoroughly and in a scientific manner. Tourism safety and security are too important not to be the subjects of the best academic and professional research" (p. 1).

"Experts indicate that terrorism will continue to victimize soft targets, attacks will become more indiscriminate, terrorism will become institutionalized as a method of armed conflict, it will spread geographically and the public will witness more terrorism

than ever due to the media's improved ability to cover terrorist incidents" (Sonmez, 1999, p. 3).

The vast contribution of tourism to the economy is so large that any disruptions in the industry are cause for concern. Any economic downturn extends beyond the tourism industry itself to include airlines, hotels and catering, and to businesses that supply intermediate or final goods which tourists purchase. In other words, virtually all facets of the economy are affected (Essner, 2003).

Tourists' Perceptions

The tourism industry is highly sensitive to sudden economic events and perceived danger can be catastrophic for the industry. Thus, perceived safety is the dominant factor for its continued growth. Fixed locations such as hotels, convention centers, restaurants, and theme parks are the most vulnerable to attack. Risk of terror attack is now a long-term implication of the tourism industry that must be dealt with to ensure patron confidence (Gold, 2003). Following the Bali bombing of 2002, tourist arrivals to that location fell forty percent (LaMoshi, 2003). According to Travel Industry Association research prior to the 9/11 attacks, fifteen percent of tourists view safety as the most important facet of travel. Even companies have restricted travel of employees due to safety concerns. Based on this research and since the 9/11 attacks, Disneyland moved swiftly to add security measures such as increased security patrols, patron inspections at the gate, limiting the number of access points, and tighter ID controls. Now, Orange County California law enforcement agencies meet with convention planners, hotel operators and tour operators to discuss security issues and provide bomb-sniffing dogs for security enhancement (Cain, 2002).

To illustrate the power of perception, terrorists now realize they can have an effect on people with mere threats, thus providing them with a pseudo psychological victory. Government officials must also be mindful of comments that can be exaggerated and cause increased fear unnecessarily. The media plays a huge role in perception with sensationalism of reporting (Alexander, 2002).

In the aftermath of 9/11, the airline industry moved to instill confidence in the traveling public. A step up in security to bring back positive perception was accomplished through implementing surveillance cameras in public view, performing background checks on employees and passengers, along with other activities openly seen by the public (Hall, 2003). There are two overall strategies that can be effective in creating a safe atmosphere for tourism. The first is a passive approach that is comprised of hardening of potential terrorist targets through increased security personnel, more stringent patron scrutiny, and the implementation of on-site security systems. The second is an active approach that involves the use of overwhelming law enforcement technologies such as the monitoring of groups associated with terrorism, pooling and analyzing intelligence information, preemptive surveillance, search and seizure, interrogation, detention, and prosecution when plans for attack are discovered (Netanyahu, 2001).

In order to counter the threat of terrorism and to put minds at ease, the World Travel & Tourism Council based in the United Kingdom announced that it has developed a Security Action Plan. The purpose was to publicly announce initiatives to be implemented by the tourism industry stating that experience shows that once an immediate threat has lifted, people's enthusiasm to travel rapidly returns. The

approach is to develop a foundation of practical measures that can be utilized to reduce the effects of terrorism, including the convincing of the public that the tourism industry must accept the risk of terrorism and is attempting to reduce that risk (Travel & tourism, 2003).

World Travel & Tourism Council

In an initiative to reach out to the entire industry, the World Travel & Tourism Council (WTTC) announced the development of the Travel & Tourism Security Action Plan in which they state the responsibility of security is primarily that of the government. However, the private sector can play an important role in the protection of customers and employees. The WTTC plan calls for cooperation among all stakeholders, both public and private, and effective relationships meaning there should be no rivalry between competitors when it comes to security issues. "Security is a strictly non-competitive issue and requires stakeholders to work together, adhering to the general guidelines promoted through this Action Plan and sharing crucial information freely with each other" (Travel & tourism, 2003, p. 4). "A comprehensive set of working principles and operating measures are outlined in the plan, which collectively provide a frame of reference, helping to guide the development of security initiatives across all sectors of the industry and government" (Travel & tourism, 2003, p. 4). There are four key principles of the WTTC's Security Action Plan.

1. Coordinate all policy, actions and communications. This will help create a spirit of cooperation among all employees, working partners and other stakeholders, as well as integrating security into all policy and operational

areas. It is important that relationships between stakeholders are established at the earliest opportunity and are constantly maintained. The public sector is responsible for ensuring that effective conduits of communication are established for security coordination (Travel & tourism, 2003, p. 5).

2. Secure operating environments. It is a government responsibility to identify and highlight areas of security concern within national borders and to set the broad criteria when establishing measures appropriate for general and specific threats. The basis of creating a secure environment lies in the development of a sound security plan. Every enterprise must have its own security plan, which must never be a direct template transferred from one scenario to another. Although many of the procedures and much of the terminology may be the same – and can and should be replicated for commonality of practice and ease of communication (Travel & tourism, 2003, p. 7)**.**
3. Aim to deny terrorists freedom of action. Travel & Tourism enterprises must make contact with and engage as wide a cross section of the host community as possible, including those not directly affected by their operations. Without engagement – winning hearts and minds beyond the immediate confines of an enterprise - managers will have little feel for the prevailing regional and local ground currents, which are likely to be the first indicators of an increased threat. It is essential that industry stakeholders institute a system for assessing whether potential employees are likely to prove security risks (Travel & tourism, 2003, p. 9).

4. Access and work with the best intelligence. The gathering of intelligence, defined as the processing of raw data into usable information, must be subject to constant review and amendment as new information is received. It is best described, therefore, as a cycle: collection, processing, dissemination, and direction. The Travel & Tourism industry must develop a coordinated and structured approach to meet each of these four stages, exploiting to the full areas of internal strength, notably its in built capacity for the collection of local intelligence, and referring to the public sector in areas of weakness, such as the processing of that information (Travel & tourism, 2003, p. 9).

Regardless of the blurred lines of responsibility between the private and public sectors, the private sector has the responsibility of protecting customers and employees. The stifling of cooperation among all stakeholders can only impede progress for the greater good. The WTTC plan provides for an initiative to develop broad security plans among all sectors of tourism allowing each entity to decide the details best suited for their own environment. The four key components to consider are coordination, secure environments, denying freedom of action to terrorists and use of the best intelligence.

Department of Homeland Security

In contrast to the plan put forth by the WTTC and as part of an overarching strategy to mobilize and organize the nation in protecting against terrorist attack, in 2003 the Department of Homeland Security (DHS) published, “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.” This was an effort to facilitate the strategic planning process amongst the private and public sectors.

In this eighty-two page document, many different industries and entities are discussed; however, the tourism industry as a whole is not mentioned. In fact, there is only one mention of tourism in the entire document. When deciding key assets, our national monuments are designated to a category of their own. "The sites and structures that make up this key asset category typically draw large amounts of tourism and frequent media attention – factors that impose additional protection challenges" (U.S. Department of Homeland Security, p.71).

Though the tourism industry is not specifically mentioned in the document, the theme of safeguarding against terror attacks is congruent with this study. The DHS states its eight guiding principles in the development of the national strategy:

1. Assure public safety, public confidence, and services;
2. Establish responsibility and accountability;
3. Encourage and facilitate partnering among all levels of government and between government and industry;
4. Encourage market solutions wherever possible and compensate for market failure with focused government intervention;
5. Facilitate meaningful information sharing;
6. Foster international cooperation;
7. Develop technologies and expertise to combat terrorist threats; and
8. Safeguard privacy and constitutional freedoms (U.S. Department of Homeland Security, 2003, p. ix).

The tourism industry has little influence on security agendas although security agendas have far reaching affects on tourism (Hall, 2003). Yet, few tourist attractions are

ready to combat the threat of terrorism (Tarlow, 2002). The Department of Homeland Security posits that the private sector, which would include tourism, is its own first line of defense. Therefore, those operating in the private sector must continually reassess and adjust action plans in order to address the increased risk presented by deliberate acts of terrorism (U.S. Department of Homeland Security, 2003).

Clearly, the DHS views its role as that of an information gathering and sharing entity. Their approach to security for the private sector is to encourage overall goals and objectives for each organization to strive to accomplish. Their position is that the country's assets are vast and highly complex and if they concentrate all efforts on one sector, then the terrorists will focus on targets that are less protected. Therefore the federal government will work with state and local governments and the private sector to develop methodology to focus on high-priority activities and approaches to counter the threat of terror attack. A stated objective is to assure protection of targets that face an imminent threat. A clear example is the threat of terrorism that the tourism industry must recognize as a threat. It should be noted that tourism is not mentioned as part of the government's overall plan, but that the private sector must collaborate and cooperate within itself to provide focused protection against the anticipated threat (U.S. Department of Homeland Security, 2003).

The comprehensive approach begins with the availability of relevant expertise and access to affordable tools and best practices that will encourage the private sector to take immediate action at all levels of the risk management component. Thus, the coordinating of information dissemination between the government and the tourism industry is of utmost importance for effective decision-making. It is imperative to have in place

processes and systems for communication and exchange of crucial security-related information among the private sector operators establishing a foundation for cooperation (U.S. Department of Homeland Security, 2003).

Regarding personnel issues, the DHS provides four areas that employers must address. First, employers must prevent an insider from conducting sabotage. That means not only employees, but also anyone who has access such as contractors, outsourced service providers, and even temporary help. Second, recruit and train more skilled personnel to protect assets. Security personnel must be trustworthy, reliable, and properly trained. Third, ensure personnel are secure in the work place to do their jobs. And finally implement communication programs to manage risk in a constructive manner. A culture of protection awareness is very effective in the workplace where everyone is on guard for a terrorist attack (U.S. Department of Homeland Security, 2003).

While ongoing research and development is contributing the latest technologies to combat terrorism, the DHS assigns responsibility to the private sector for identifying standards, tools, and processes to establish research priorities. The challenge for the tourism industry is for individual stakeholders to identify commonality among needs and coordinate research and development activities that will produce the greatest return in the interest of all (U.S. Department of Homeland Security, 2003).

In the document, the DHS places a great emphasis on modeling, simulation, and analysis as a means to evaluate the risks of a particular vulnerability and make better decisions regarding protection. As a real-time decision tool, scenario training can help reduce the effects of a terror attack and prevent secondary attacks. The private sector has

a long history of dealing with natural disasters, but a lack of experience in planning and contending with the threat of terrorism. Since no long-term historical data is available to evaluate patterns or behaviors, no evidence exists as to which strategies would be most effective in deterring terror attacks (U.S. Department of Homeland Security, 2003).

Demand for studies in this area will be great and priorities among projects will need to be established to give the most common benefits and recognize the greatest threats and vulnerabilities. This includes an effort to enhance data collection and standardization. Data related to protection strategies may not exist, be accessible, or be available in a standardized format These processes, systems and standards will need to be created so model data sets can be utilized (U.S. Department of Homeland Security, 2003).

The approach of the DHS in defense of national monuments against terror attacks can easily be transposed to address the same concerns within the tourism industry. The large attraction associated with national monument sites makes apparent the potential for human loss resulting from terrorism. A proactive approach in protection of these facilities is important regarding human life as well as preserving public confidence. To address concerns, the DHS specifies numerous initiatives that the Department of Interior (DOI) shall implement in the protection of sites.

- Define criticality criteria for national monuments, icons, and symbols. DOI will work in concert with DHS to develop specific guidance to define criteria and standards for determining the criticalities and protection priorities for our national monuments, icons, and symbols.
- Conduct threat and vulnerability assessments. DOI will work in concert with DHS and other appropriate authorities to conduct threat and vulnerability

assessments to identify gaps in visitor protection processes as well as asset protection.

- Retain a quality security force. DOI will explore alternatives to foster efforts to recruit, train, and retain a skilled and motivated security force.
- Conduct security-focused public outreach and awareness programs. DOI will enlist public support in the protection of our national icons and symbols through sustained public outreach and awareness programs.
- Collaborate with state and local governments and private foundations to assure the protection of symbols and icons outside the federal domain. DOI will work with state and local governments and private institutions to explore alternatives to protect symbols and icons such as historical buildings and landmarks that are outside the purview of the federal government.
- Evaluate innovative technologies. DOI, in concert with DHS and other key stakeholders, will explore ways to employ security technologies to ensure the protection of visitors to monuments and other like attractions.
- Make provisions for extra security during high-profile events. DOI will work with law enforcement agencies to manage visitor periods at national monuments and provide extra security during high-profile events taking place in or around national icons (U.S. Department of Homeland Security, 2003, p. 33).

The DHS insists that terrorist can and will attack the United States. The vast majority of the complex and diverse target sets within the U.S. are controlled by the private sector. It is imperative that the comprehensive strategies put forth by the

Department of Homeland Security be implemented. The DHS states they will be working to identify options to compensate those in the private sector for implementing security enhancements as an incentive to be proactive. That means rewarding those in their industry for being leaders on security issues (U.S. Department of Homeland Security, 2003).

The WTTC and the DHS have both stated the vast need in planning strategies to thwart terrorism where populations are attracted to congregate. Calhoun and Weston (2003) provide a model for proactive prediction of human violence. This body of literature makes clear the need to be proactive in the endeavor to protect against terrorism. What is lacking in the literature is information on detailed strategies that are effective and feasible to be utilized by the tourism industry. To obtain such information, subject matter experts (SME's) must be queried and the process of data collection, analysis and dissemination put into action for the private sector. Clearly it has been stated the sharing of information and cooperation uninhibited by competition is paramount.

Contemporary Threat Management

After studying countless cases of intended violence directed at an array of individuals and groups, Calhoun and Weston developed the concept of contemporary threat management (2003). Their work establishes a link, not among the targets, but in the fact that violence was intended by the perpetrators against those targets. Professions involving human interactions cannot ignore experiences drawn from contemporary threat management. Research information is too vast for anyone to hide behind the excuse of ignorance.

Contemporary threat management posits those intended on committing violence exhibit a set of recognizable behaviors. This includes perpetrators who target individuals because of who they are or what they represent. The cornerstone of their work is the repetitive observations of experienced employees who recognized patterns of behavior in individuals leading up to violent acts. Throughout their work, Calhoun and Weston (2003) demonstrate that a proactive approach to reducing threat is the most effective model.

A vast historical body of research exists on intended human violence. From school shootings to public figure assassinations, the researchers have covered the gamut. No practical advice was born out of the research in the way of recognizing signs of intended violence prior to the act. Impractical research offered little use to law enforcement in identifying, assessing, and managing those approaching a violent intent. Such inept research produced results that noted domestic abusers often took hostages. Law enforcement waiting for a hostage situation is completely reactive and unproductive. The purpose of the threat management process is to provide tools for identifying, assessing, and managing individuals before the violent act occurs (Calhoun & Weston, 2003).

Actuarial tables are sophisticated client profiles used by insurance companies to accurately predict risk among certain groups of individuals. Actuarial profiles allow insurance companies to turn a profit in that high risk groups have higher premiums to offset the cost of claims. In law enforcement terms, actuarial tables are synonymous with criminal profiling. This is not helpful to threat managers because there are built in expectations and generalities that can cause individual case evidence to be

overlooked. For example, the D.C. sniper case profile experts in the media told the public that the sniper would turn out to be a lone white male in his thirties who had relationship issues with women, had a military background, and had been fired from a craft/ hobby store. Of course it turned out to be two black males many years apart in age. The one with a military background was not the shooter. The rest of the espoused profile was inaccurate. Attempts to use profiles are dangerous causing specifics to the case to be overlooked (Calhoun & Weston, 2003).

The Calhoun and Weston model is based on behaviors of the violent perpetrator. Behaviors assessed as a whole on a two way path, up or down the behavior escalator that can result in a violent act. The model requires the continued monitoring of an individual's actions which in turn provides threat managers with a set of predictive indicators (Calhoun & Weston, 2003).

Although the threat management process has a place in the tourism industry, what's important to note for the present study is the recognition that a proactive approach to violence is most effective in protection of life.

Delphi Approach to Research

In order to obtain and describe the sought information from subject matter experts who are separated by geographical distance; a Delphi research model can be effective. The legitimacy of the Delphi for conducting research in this study shall be discussed in this section. Also, a description of its structure will explain the appropriateness of the Delphi as a method of research for the research questions of this present study.

In the early 1950's, the Rand Corporation conducted a study sponsored by the Air Force entitled "Project Delphi." The purpose of the study was to obtain a consensus of opinion among experts through the use of questionnaires built on top of one another with controlled feedback features (Linstone & Turoff, 1979). Subsequently, various fields of study have taken advantage of the Delphi method to develop policy and planning, determine the future structure of hospitals, and determine scenarios most likely to occur in social services and healthcare (Adler & Ziglio, 1996).

The Policy Delphi produces non-numeric, verbal data. It is used to establish all the differing opinions of experts and the pros and cons of each position. Later, the decision makers can utilize the ranking of ideas by the panel members to formulate policies or take action (Turoff, 1970). This fits the purpose of this study in that many strategies are offered to combat terrorism. Decision makers will be able to use the results of the study while being made aware of the expressed barriers to implementation of individual strategies. There are four possible objectives for any Delphi study.

1. To explore or expose underlying assumptions or information leading to differing judgments.
2. To seek out information that may generate a consensus of judgment on the part of the respondent group.
3. To correlate informed judgments on a topic spanning a wide range of disciplines.
4. To educate the respondent group as to the diverse and interrelated aspects of the topic.

A combination of any one of these objectives can be sought as a means for soliciting interpretations, predictions, or recommendations (Turoff, 1970).

> Delphi may be characterized as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem (Linstone & Turoff, 1979, p.3).

An advantage of the Delphi method is that it allows a group of experts separated by geographical distance to participate in group communication and systematically address a complex problem or task. This is important when there is insufficient information upon which to base a decision because the best possible insights of experts can be obtained (Adler & Ziglio, 1996). Furthermore, the Delphi method allows avoiding certain disadvantages of face to face group interaction such as the bandwagon tendency, deference to the most prestigious or powerful member of the group, the vulnerability to manipulation, and the reluctance on the part of individuals to change their minds in front of others (Isaac & Michaels, 1990).

The Delphi method first involves the identification of the group or experts whose opinions are sought. Then a questionnaire is circulated to obtain each group member's list of ideas regarding the topic of the study. Next, the first round results are shared with the individual members of the group who then expand on the presented ideas or can change their position. Finally, the results are listed in random order and the panel members are asked to rate or rank the items along with any dissent a member may have for a particular idea (Isaac & Michaels, 1990).

Among the various scenarios in which a Delphi study is appropriate, the most significant for this research in when the problem being studied would benefit most from the consideration of many viewpoints and the Delphi method can facilitate discussion (Adler & Ziglio, 1996). Among the many applicable arenas for the Delphi, Linstone and Turoff (1979) specifically point out the structuring of a model, the pros and cons of potential policy options, and planning. Therefore, considering the literature review of the Delphi method, it should be considered a legitimate research technique to facilitate discussion among subject matter experts who otherwise would not be able to communicate due to geographical barriers and when there is little historical information on the subject being researched.

Summary of Review of Literature

It is more important to understand the phenomenon of terrorism than to define it. Groups of terrorists will use any means to accomplish their goals, including mass murder as a weapon (Dershowitz, 2002, p. 6). Risk managers must understand the differences in dealing with terrorism compared to criminal activity (Tarlow, 2002). The connection between tourism and terrorism is irrefutable. The tourism industry must recognize that it is a target for terror attack. Terrorists have demonstrated their ability and willingness to attack within the United States.

This review has demonstrated a gap in the literature regarding the specific types of security strategies needed to be implemented in the tourism industry along with associated barriers to implementation. It has also shown the need for academic research in the tourism security arena and furthermore, the need for a set of specific guidelines on security strategies.

Finally, it has been pointed out that the Delphi method is an effective and appropriate manner in which to collect data and conduct research.

CHAPTER III

METHODOLOGY

The purpose of this study was to gather strategies and factors from tourism security professionals in order to formulate comments from which terrorism risk management policies can be developed. There was an attempt to correlate views and opinions regarding terrorism risk management and to allow respondents to react to and examine opposing viewpoints. The intent of this study was to put forth all possible options for consideration by individual, corporate, and agency policy makers. Also, criticality and barriers to implementation of any particular strategy as well as examination of the acceptability of any particular strategy was included. The purpose of this study is not to make decisions for policy makers, but rather, to provide all available options presented by an informed group for consideration by policy makers.

Research Model

The literature review pointed out the need for academic, government, and private sector cooperation and the need to exchange ideas to address the threat of terrorism in the tourism industry. The issue is not only a local problem, but must be dealt with on a national level. In a comparison study of four different questionnaire methods, Presser and Blair (1994) established that an expert panel was more efficient in cost and productivity than the other methods. This study utilized the Delphi technique in order to provide structure for the group process. The Delphi technique administered via email thwarts the barrier of financial and time constraints associated with travel and allow geographically dispersed subject matter experts to participate from their respective locations (Turoff & Hiltz, 1996).

The Delphi technique allows for interaction with group members whose opinions are sought on an individual and anonymous basis. The collected feedback of each questionnaire is provided individually to each panel member so they can reconsider their position and critique others' without the disadvantage of face-to-face group interaction (Linstone & Turoff, 1979).

When working toward policy decisions, the objectives of a Delphi are a combination of discovering all possible options for consideration, estimateing impact and consequences of each option, and determining acceptability of any option. The overall goal is not one of creating consensus as much as it is to expose all ideas and strategies and the pro and con arguments for each (Linstone & Turoff, 1979). Weaver (1971) states the Delphi best serves when establishing priorities in development of planning tools. Pill (1971) also concluded the Delphi was useful in long range planning where results were not immediately available.

This Delphi study collected data in the form of verbal statements and comments. As such, a rating system had to be developed that could evaluate the positions of group members pertaining to importance and feasibility of the various ideas. A scale was utilized to provide some reasonable assurance that respondents would make compatible distinctions between the concepts available to choose from on the Likert scale (Linstone & Turoff, 1979).

Population

The sample consisted of subject matter experts who matched the definition of "tourism security professional" for the purpose of this study. The operational definition of tourism security professional is an individual who has both academic and applied

knowledge in the tourism security field. To be a professional, one has to have worked in the field and had his/her work reviewed by peers.

The Delphi method requires the assembly of an expert panel to whom a series of questionnaires shall be given. A core group of subject matter experts was gathered through a literature search, professional organization listings, and professional conference rosters as modified from the Peter Williams study. Those in the core group were contacted and asked to nominate peers they believed to fit the criteria discussed above (Williams, 2000).

A core group of twelve subject matter experts (SME's) was developed and contacted via email. They were sent an information sheet (see Appendix A) that described the study and expectations of participants and were asked to nominate individuals whom they believed to be credible experts in the field of tourism security. This resulted in a list of seventy-six names including the original twelve from the core group. All seventy-six were contacted via email and asked to participate in the study. Thirty-three responded and agreed to participate. Twenty-four participated in round one. Twelve successfully completed round two. The original thirty-three that agreed to participate in the study were invited to participate in round three. Twelve participants successfully completed the round three questionnaires.

All communication with the panel was conducted via electronic mail. Participants were contacted at the beginning of each round via email and periodically during each round to encourage the timely completion of the questionnaires.

Procedure

This study was a Delphi that utilized electronic mail as the means to distribute questionnaires, collect data, and communicate with the panel members. An important aspect of the Delphi via the computer format is the consistent participant contact. The feedback process enables participants to respond throughout its entirety and provides closure upon completion. This further enhances the quality of the study since the participants are not locked into responding only during the individual rounds (Turoff & Hiltz, 1996). The first step is to choose participants and ask them for additional nominees to participate. A total of ten to fifteen participants is sufficient for a single group to be represented. The group should be contacted and told the purpose of the study, the type of study, the composition of the panel and how the results will be shared. When the first questionnaire is sent, it should be preceded with a cover letter. A second letter can be sent to encourage the participants to make a timely response (Gilmore & Campbell, 2004).

In this present study, the panel was assembled by using the process described in the section on population. There were three rounds of questionnaires. The first round was exploratory, in that the questionnaire provided an open-ended question that sought from the expert panel what ideas or strategies could be implemented in the tourism industry to reduce the chance of a terror attack. For the complete invitation and cover letter see Appendix A. The complete round one questionnaire can be found in Appendix B. The responses from all respondents were compiled into a comprehensive list of strategies and techniques the experts proposed to reduce the propensity for terror attacks in the tourism industry. Gilmore & Campbell (2004) posit that after the first round, the researcher

should synthesize and analyze the responses. A master list should be compiled for ease of analysis. This list should be distributed to the panel for clarification and the final list should be summarized in clear and concise statements.

The complete list of strategies that was developed in the first round of this study was shared in a second round instrument to the panel. Refer to Appendix C for the second round instrument. In the second round of the Delphi, each member of the panel is asked to rate or rank the items in the master list (Isaac & Michael, 1997). In the present study, the panel was asked to further clarify each idea discussing its strengths and weaknesses and to rate the feasibility of each item on a Likert scale. And following each strategy or idea, the panel was asked to state any barriers to implementing the particular strategy within the tourism industry. Any new ideas that resulted during the second round were given the same treatment as previously stated ideas. The average feasibility rating of implementation for each strategy was calculated. The comments from the panel were assembled regarding strengths, weaknesses, and barriers to implementation for each idea and assimilated into the master list of strategies.

The information requested in the second round was added to the master list in preparation for the third round. Isaac & Michael (1997) state that in the third round, the respondents will begin to see any trends that are developing within the group. They should be asked to rate or rank the items on the list for a second time. This latest ranking along with any comments should be presented to the group as the final statement. In the present study, the third round utilized the results of the second round and asked the panel to rank the list of strategies from most critical to the least critical in regards to the effect that the strategy will have in decreasing the chance of a terrorist attack. See the complete

questionnaire in Appendix D. The average ranking of all strategies was calculated. The rankings were correlated with the feasibility ratings and placed accordingly in a criticality-feasibility matrix. Each quadrant of the matrix was assigned a priority level for ease of discussion.

Instrument

A Delphi technique survey instrument with open-ended questions was used to produce verbal data in the first round. There was additional space after each idea that was listed for the respondent to discuss the strengths and weaknesses of the particular idea. The purpose of the first round was to collect as many ideas as possible from the respondents regarding the reduction for propensity of terror attack. See Appendix B for the round one instrument.

The second round survey utilized an instrument designed to solicit a rating of the compilation of responses from the first round. Using a Likert scale for the participants to respond, the questionnaire derived information about the opinions of professionals as to the feasibility of each idea proposed by the panel. A neutral response was not available on the scale as this would provide no useful information (Linstone & Turoff, 1979). During this round, the study sought more descriptive data as panel members were asked to list the barriers to implementation of each strategy. This was an opportunity for panel members to critique the ideas of other panel members with anonymity. See Appendix C for the complete second round instrument.

The third round instrument listed the results of the second round in random order and asked the panel to rank the list of strategies from most critical to the least. See Appendix D for the round three instrument.

Design and Statistics

This was a basic descriptive and exploratory study using the Delphi technique to gather strategies and factors from tourism security professionals in order to formulate comments from which terrorism risk management policies can be developed. The Delphi process consisted of three rounds of data collection utilizing a panel of subject matter experts. After the first round, each subsequent round disseminated the data from the proceeding round to each member of the panel, followed by the questionnaire for the current round. All questionnaires and communications were conducted via electronic mail.

Seventy-six tourism security experts were invited to participate in the study and were sent invitation via email on April 19, 2004 (see Appendix A). They were sent via email the official university information sheet and consent form along with instructions to complete the first round questionnaire. Thirty-three responded and agreed to participate. Reminders were sent on May 23rd, July 9th, and September 14th. The first round was ended on October 1, 2004. Twenty-four group members participated in round one.

The second round began on November 2, 2004 with an invitation being sent to the original thirty-three experts who agreed to participate. The first round instrument generated fifty-four separate ideas or strategies that were included in the round two instrument. The round two questionnaire asked the participants to provide strengths and weaknesses to each strategy and to rate each strategy as to its feasibility using the provided scale. Each participant was asked to provide the number of years experience in the field. A reminder email was sent on December 2, 2004. On January 10, 2005 the

second round was ended with a total of twelve group members successfully completing the round two instrument.

The original thirty-three that agreed to participate in the study were invited to participate in round three that began on January 17, 2005. In the third round instrument all the ideas from the previous rounds were provided to the participants who were asked to rank the ideas from the most critical to the least critical. A reminder was sent on February 1, 2005 and the round was completed on February 10, 2005. Twelve participants successfully completed the round three questionnaires.

CHAPTER IV

ANALYSIS OF DATA

This descriptive study was designed to develop a prototype guideline for the tourism industry from which security personnel and risk managers can formulate policies and procedures in an attempt to reduce the likelihood of a terrorist attack. A total of fifty-four strategies were the result of three rounds of questionnaires distributed to subject matter experts. The following chapter will place those strategies in formats from which the reader can gain understanding of the findings.

In addition to the strategies developed by the study, recommendations regarding criticality and feasibility are discussed as well as any barriers to implementation of various strategies. And the following research questions will be addressed:

1. What are the needs of the Tourism Industry to reduce the risk of terrorist attack?
2. What are the solutions to the stated needs?
3. What are the barriers to the stated solutions?
4. What are the prototype guidelines to apply the solutions to the stated needs?

Finally, a discussion of ancillary findings will be brought forth.

Identified Strategies to Reduce Terror Attacks

This section is intended to address the first research question: What are the needs of the Tourism Industry to reduce the risk of terrorist attack? In order to answer the question, the first round questionnaire asked the panel of experts “What actions can be taken at events and locations (hotels, resorts, theme parks, convention centers, public gatherings, etc.) frequented by tourists that could reduce the propensity for terror

attacks?" The result was a comprehensive list of fifty-four strategies to be implemented by various operating businesses within the tourism sector as seen in Table 2.

Table 2

Detail List of Fifty-Four Strategies to Reduce Terror Attacks

Strategy #1	Terrorism only works due to media. National government needs to have agreements with media regarding a terrorist attack; much the same way they control war footage.
Strategy #2	Additional training provided to teach first responders about terrorist goals and their role in limiting the success of a terrorist attack (i.e. what to do after the scene is stabilized).
Strategy #3	Make non-vital targets more readily available in order to channel terrorist activity to those locations. Ensure non-vital targets are politically acceptable.
Strategy #4	Publicize as many events as possible as being multi-national. Tourism must be advertised for success. Use of in-place marketing systems to stress diversity will create additional considerations for terrorist in planning an attack.
Strategy #5	Train event and safety specialists in dynamic as opposed to static security techniques. Utilize diverse and randomized methods for screening tourists upon entry to an event and for controlling crowd flow during an event. Where warranted bag, purse, and package checks of guests, participants, invitees, and employees.
Strategy #6	Design increasing layers of security around an event based upon a risk assessment. In line with dynamic techniques, make heavy use of a double entrance approach; it will be difficult for terrorists to breach if they are unsure what measures will be in place after the initial entrance. Any persons attempting to leave after the first entrance and before the second entrance would be considered suspect.
Strategy #7	Improve physical design of facilities to take into account the terrorist threat. Design new facilities with crime prevention in mind. Remodel existing facilities with crime prevention in mind.
Strategy #8	Have a unified method to determine risks.
Strategy #9	Reach out to the community for intelligence. Establish communication between hotels, parks, and other events with local and federal law enforcement.

Table 2 (continued)

Strategy #10	Having community leaders, including religious leaders, speak out in a unified voice against terrorism since most recent acts of terrorism are based on some slanted view of religion.
Strategy #11	Ask the media's cooperation in correctly portraying these people. They are not suicide bombers, but homicide bombers, they are not freedom fighters, but murderers, and they are not to be admired, but scorned.
Strategy #12	Network with other communities to determine what programs have bee successful in combating terrorism.
Strategy #13	Implement a crisis management plan. Conduct threat assessments for special events and structures to include integrated response plans involving private and public first responders.
Strategy #14	Improve intelligence gathering, analysis, and sharing capabilities among private and public security professionals.
Strategy #15	Where applicable, personal screening of guests, participates, invitees, and employees should be conducted.
Strategy #16	Conduct thorough background and credit checks on each employee.
Strategy #17	Outside contractors for the event or location should have backgrounds conducted on own employees by third party.
Strategy #18	All employees should have identifying badges and/or tags.
Strategy #19	All working contractors should be provided with a contractor's Id tag or badge.
Strategy #20	All employees should come through security check point and verified that they are an active employee.
Strategy #21	All contractors should have a specific parking area and be subject to vehicle screening by security personnel.
Strategy #22	Frequent and high profile public service announcements regarding suspicious activities in or near venue, i.e. patrons should maintain control of their belongings.
Strategy #23	Implement the utilization of closed circuit television in tourist areas at venue and core surrounding area.
Strategy #24	Deploy plainclothes law enforcement personnel to detect and obtain critical information from within the crowds. Personnel can be used for intelligence gathering and counter surveillance engagement.

Table 2 (continued)

Strategy #25	Utilize special security units that provide confidence to visitors (Examples: Bike patrols, Mounted Units, Motorcycle Units).
Strategy #26	Increase cooperative effort/ commitment with federal, state and municipal entities.
Strategy #27	Train personnel (both police and private sector) in recognizing potential threats and actions that warrant police intervention A training program that empowers every employee to be a security agent.
Strategy #28	Train, equip, and staff police personnel with CBRNE gear.
Strategy #29	Target-harden venues to include metal detectors.
Strategy #30	Stage specially trained law enforcement personnel for bomb intervention near the venue. Train staff and deploy personnel in bomb detection/suppression. Deploy mechanical bomb detection devices with police and private sector security staff.
Strategy #31	Fund, budget, and deploy air unit support to monitor event.
Strategy #32	Billboards with instructions on what to do if a crisis occurs. People should always know where they are and where they are going or where they need to go.
Strategy #33	Implement the utilization of face recognition software in tourist areas.
Strategy #34	High visibility of law enforcement personnel for a deterrent aspect.
Strategy #35	Enhance security procedures to include the use of manual and electronic search methods.
Strategy #36	Utilize citizen patrols that have been specifically trained to enhance security or law enforcement.
Strategy #37	Plan with the local police department.
Strategy #38	Ask your guests to be aware. Don't scare them. Tell them their stay will be more enjoyable if they are aware of their surroundings and take simple precautions to keep them and their belongings safe.
Strategy #39	Partner with the media to publish safety tips and location maps.
Strategy #40	Use of trained dogs to detect weapons/ contraband. Deploy K9 units to assist in bomb detection.
Strategy #41	Use training drills to prevent skill decay. Train and retrain.

Table 2 (continued)

Strategy #42	Recognize you (tourism venue) are a target.
Strategy #43	Tighten-up security at loading dock operations at large venues. Only allow access to those on check lists. Implement standard operating procedures for delivery. Any and all delivery vehicles should be recorded and driver's license should be recorded.
Strategy #44	Have regularly scheduled meetings with area venues to keep them informed of changing trends in security and to allow them a voice to express their concerns.
Strategy #45	Local law enforcement should become involved in organizations and serve on boards when appropriate or when asked to do so; i.e. hotel and lodging associations, convention and visitors bureaus, chamber of commerce, etc.
Strategy #46	Use barricades to prevent vehicular intrusion. Employ concrete barriers and spike strips. Keep vehicles at a distance from the perimeter.
Strategy #47	Cross communicate with local and fed law enforcement on updated terrorist intelligence.
Strategy #48	Utilize off-hour perimeter security patrols at gates and fences. All outer perimeters should be patrolled on a regular unscheduled time span.
Strategy #49	Provide ongoing training for security personnel on terrorists' activity and tactics.
Strategy #50	Employ cameras with a big screen picture of people walking in and around specific strategic areas of interest. Similar to radar trailers; "Do you see how fast you are driving?"
Strategy #51	Use photo identification and personalized security devices (i.e. ID cards, bracelets, etc.) for patrons.
Strategy #52	Install motion detectors that are voice activated and state something to the effect that the premise is under law enforcement surveillance.
Strategy #53	Require advanced reservations to access vital places. Scan cards are mailed to allow access to the event.
Strategy #54	Use radioactive material detection devices throughout facilities or event areas.

Solutions and Implementation

The second research question asks, "What are the solutions to the stated needs?" The third research question asks, "What are the barriers to the stated solutions?" To address these questions, a foundation is established with the fifty-four proposed strategies. The strategies clearly establish what experts describe as needing to be done to reduce the chance of a terror attack, however implementing those strategies as a solution is too simple. Each strategy brings ramifications and repercussions of its own. In order to formulate solutions, more information must be obtained. To bring forth this information, a second round questionnaire was distributed to the expert panel. This second questionnaire was constructed by providing the comprehensive list of fifty-four strategies to the expert panel. The complete second round instrument can be found in Appendix C. The panel was asked to review the list and provide their insight into each individual strategy. Specifically, the panel was asked to provide comments for each strategy regarding its strengths and weaknesses and any barriers to implementation. Also, the panel was asked to rate each strategy as to how feasible it would be to implement. Table 3 represents the Likert scale used for the feasibility rating. For the complete questionnaire see Appendix C.

Table 3**.**
Representation of Round Two Questionnaire Likert Scale

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

The feasibility rating for each strategy from the individual panel members was collected and placed in Table 4 below.

Table 4

Feasibility Rating of Fifty-four Proposed Strategies by SME (Listed by strategy number, Most Feasible = 1, Least Feasible = 4)

Strategies listed one through fifty-four	SME Code Number												Strategy Average Rating
	1	2	3	4	5	6	7	8	9	10	11	12	
1	4	3	3	3	4	3	3	4	3	4	4	3	3.83
2	2	2	2	2	1	2	2	2	1	2	2	2	1.83
3	3	4	3	3	4	3	2	4	4	3	3	3	3.08
4	4	3	3	3	4	2	1	1	3	2	3	3	2.67
5	2	3	2	2	1	2	2	2	3	2	2	2	2.08
6	2	3	3	3	1	2	2	2	4	3	2	3	2.50
7	2	2	3	2	2	2	2	2	3	2	2	2	2.17
8	1	3	3	2	2	3	4	2	4	2	3	1	2.25
9	4	3	2	3	2	2	1	1	2	2	3	2	2.25
10	1	3	4	3	4	4	3	2	3	2	3	3	2.83
11	3	3	4	4	4	3	3	3	4	4	4	3	3.50
12	2	2	1	2	1	1	1	1	1	2	1	1	1.33
13	1	1	1	2	1	1	1	1	2	1	2	1	1.25
14	4	2	2	2	2	1	2	2	2	2	2	2	2.08
15	3	2	2	2	2	1	2	4	3	2	1	2	2.17
16	2	2	2	2	2	3	1	2	2	2	1	2	1.92
17	3	2	2	1	4	3	2	1	1	2	2	2	2.17
18	2	2	1	3	2	1	1	1	2	1	1	1	1.50
19	2	1	1	2	2	1	1	1	2	1	1	1	1.33
20	2	2	3	2	1	2	2	2	1	2	2	2	1.92
21	3	2	3	3	4	2	1	3	2	2	2	2	2.42
22	2	2	2	3	2	2	1	2	1	2	2	2	1.92
23	3	3	2	3	2	4	2	1	2	4	3	2	2.58
24	2	2	1	2	1	1	2	1	1	2	2	2	1.58
25	3	3	2	3	1	2	2	2	1	2	3	2	2.17
26	2	2	2	3	2	2	2	2	2	1	1	2	1.92
27	2	2	2	3	2	2	1	1	2	1	2	2	1.83
28	3	3	2	3	2	3	2	4	2	1	4	2	2.58
29	2	3	2	2	2	2	1	2	1	2	2	2	2.00
30	2	3	2	2	2	2	3	3	2	2	2	3	2.33
31	3	2	2	3	2	2	3	2	2	2	2	2	2.25
32	2	2	2	3	2	2	3	3	2	2	3	2	2.33
33	2	2	2	2	3	2	2	3	2	1	2	2	2.00
34	2	1	2	2	1	1	2	2	1	1	2	1	1.50

Table 4 (continued)

Strategies listed one through fifty-four	SME Code Number												Strategy Average Rating
	1	2	3	4	5	6	7	8	9	10	11	12	
35	2	3	2	2	2	3	2	2	4	2	2	4	2.67
36	3	4	2	3	3	4	1	2	4	3	3	4	3.00
37	2	2	3	2	2	1	2	2	3	2	2	2	2.08
38	3	2	3	2	2	3	1	2	3	4	4	3	2.67
39	3	2	3	2	1	1	2	2	2	3	2	2	2.08
40	2	2	3	2	2	2	2	1	2	1	2	2	1.92
41	3	3	2	3	2	2	2	4	4	2	2	2	2.58
42	1	1	1	1	1	2	1	1	1	1	1	1	1.08
43	1	2	1	3	2	2	3	1	1	2	1	2	1.75
44	1	2	2	1	3	2	1	2	1	3	2	2	1.83
45	3	4	3	2	3	4	1	1	2	3	4	2	2.67
46	2	2	3	4	2	2	1	2	2	3	2	2	2.25
47	2	2	1	2	2	2	3	1	3	2	4	2	2.17
48	2	2	1	2	1	2	1	2	2	1	2	2	1.67
49	4	3	1	2	3	3	2	3	4	2	4	3	2.83
50	3	2	3	2	2	3	2	4	4	3	1	2	2.58
51	2	3	2	2	3	2	2	2	1	2	2	2	2.08
52	3	2	3	3	4	4	4	2	4	4	3	2	3.17
53	3	4	3	4	4	2	1	4	1	2	3	1	2.67
54	3	2	2	4	2	2	1	2	3	2	2	2	2.25

Note: For Strategy Details See Table 2.

It was noted during analysis that the values assigned to the Likert scale needed to be reversed in order to be congruent with the ranking values. After reassigning the numeric values (Most Feasible = 1, Least Feasible = 4), the average feasibility rating for each strategy was calculated and reflected in Table 4 above.

The comments by panel members regarding the strengths and weaknesses of each strategy as well as comments pertaining to any barriers to implementation on any given strategy were collected and compiled into a usable format. These comments can be observed in Tables 7,8,9, and 10 in the next section to provide readers with what to expect when considering implementing the proposed strategies.

Prototype Guidelines

The fourth research question asks, "What are the prototype guidelines to apply the solutions to the stated needs?" An explanation of the analysis and formats for considering strategy implementation is discussed in this section. And it is in this section that a set of guidelines shall emerge. In the final round of the Delphi, the expert panel was asked to rank the comprehensive list of strategies from the most critical to the least critical. See the third round instrument in Appendix D. Once the data were collected, the average rank order of criticality of each strategy was calculated. See Table 5 below for the ranking of strategies by the SME's.

Table 5
Rank Order Score of Fifty-four Proposed Strategies by SME
(Listed by strategy code number,
Scores: 1 = most critical, 54 = least critical)

Strategy Code Number	SME Code Number												Strategy Average Score
	1	2	3	4	5	6	7	8	9	10	11	12	
1	51	39	11	26	13	45	50	5	16	27	48	34	30.42
2	1	17	10	47	8	10	24	19	7	19	7	37	17.17
3	52	40	8	3	12	18	47	42	30	15	53	52	31.00
4	42	38	1	5	17	31	24	13	20	39	50	46	27.17
5	13	11	12	46	5	8	7	12	18	13	14	6	13.75
6	41	42	46	40	41	44	39	40	47	51	49	47	43.92
7	3	10	3	1	7	6	1	3	11	12	6	7	5.83
8	4	2	25	6	3	4	26	25	12	9	10	12	11.50
9	5	5	39	2	6	5	8	14	22	11	13	10	11.67
10	8	35	40	8	10	11	14	8	13	17	24	27	17.92
11	9	37	9	4	11	9	10	11	14	4	8	13	11.58
12	10	13	14	10	9	7	9	15	6	10	11	11	10.42
13	25	3	23	48	40	22	15	18	10	24	20	14	21.83
14	6	6	13	11	4	12	12	10	8	7	15	9	9.42
15	15	14	16	44	27	26	23	24	21	16	26	24	23.00
16	14	16	4	51	14	13	16	22	23	18	18	15	18.67
17	44	44	5	17	15	43	52	21	15	40	47	51	32.83
18	17	18	6	18	16	19	17	16	9	14	16	23	15.75
19	20	19	26	19	18	17	22	20	25	26	25	21	21.50
20	16	49	27	21	25	24	25	26	49	23	29	18	27.67

Table 5 (continued)

Strategy Code Number	SME Code Number 1	2	3	4	5	6	7	8	9	10	11	12	Strategy Average Score
21	28	46	36	35	39	37	31	36	40	34	39	28	35.75
22	29	36	17	23	22	25	29	23	37	31	27	26	27.08
23	30	21	20	24	25	21	19	27	26	20	23	16	22.67
24	27	22	18	16	24	23	18	8	24	25	22	25	21.00
25	26	12	19	25	2	20	21	17	27	22	21	22	19.50
26	2	4	31	9	19	14	13	9	5	21	12	20	13.25
27	19	48	21	17	28	35	34	39	41	28	30	32	31.00
28	18	24	24	39	29	27	20	29	28	30	34	36	28.17
29	36	41	7	41	38	40	33	43	36	43	28	19	33.75
30	34	25	15	7	20	28	35	33	31	38	40	29	27.92
31	35	26	22	52	30	32	28	30	32	29	41	50	33.92
32	22	33	33	28	31	33	36	34	29	32	38	39	32.33
33	37	27	29	29	32	30	38	31	19	37	42	40	32.58
34	38	47	28	53	42	46	40	41	39	44	46	49	42.75
35	23	49	38	30	33	41	37	32	35	33	32	38	35.08
36	45	54	44	31	34	47	51	48	42	41	45	41	43.58
37	39	51	45	45	46	48	49	44	52	42	44	42	45.58
38	40	50	41	50	44	49	48	45	46	45	43	44	45.42
39	24	34	42	32	34	49	42	35	38	36	31	30	35.58
40	21	23	43	33	35	16	30	7	17	35	19	17	24.67
41	31	15	47	34	45	36	32	37	33	8	17	31	30.50
42	33	1	35	37	21	3	11	6	34	5	9	33	19.00
43	32	28	34	43	36	34	41	38	43	46	37	35	37.25
44	11	8	30	36	1	2	6	4	4	6	1	5	18.50
45	12	9	21	42	23	15	5	2	3	3	33	8	14.00
46	43	45	49	49	47	50	46	46	44	52	51	48	47.50
47	46	7	2	20	37	1	2	1	2	10	5	4	11.42
48	47	20	37	22	48	29	4	48	1	47	4	2	25.75
49	54	53	54	54	54	53	45	53	51	49	52	53	52.08
50	53	30	53	12	52	42	43	52	54	53	54	54	46.00
51	48	32	51	13	51	54	53	49	50	51	36	45	44.42
52	7	34	50	14	53	52	54	51	53	54	35	43	41.67
53	49	29	52	38	49	51	44	54	45	2	3	3	34.92
54	50	52	48	15	50	38	3	50	48	48	2	1	33.75

Note: For Strategy Details See Table 2.

In order to correlate the criticality level of each strategy with its corresponding feasibility of implementation, a criticality-feasibility matrix was devised. Using the average feasibility ratings and average criticality rankings, strategies were placed in the

appropriate quadrant of the matrix. Each quadrant of the matrix was assigned a level designated by Alpha, Beta, Chi, and Delta. For matters of discussion, every strategy can now be referred to as having a specific level of priority. Alpha level strategies are known to be of the highest criticality and the highest degree of feasibility for implementation. Likewise, Beta level strategies are highly critical, but have a low degree of feasibility for implementation. Then Chi level strategies are designated as having low criticality even though they are easily implemented. And finally, Delta level strategies are of a low critical nature with difficulty in implementation. This matrix provides for a user-friendly format for the reader to observe strategy clusters according to their criticality ranking and feasibility rating. This matrix is shown in Table 6.

Table 6
Criticality-Feasibility Matrix

Strategy numbers placed in priority levels based on average critical rank and average feasibility rating.

	High Feasibility	Low Feasibility
High Criticality	2, 12,13, 16, 18, 19, 20, 22, 24, 26, 40, 42, 44, 48 *ALPHA*	4, 5, 7, 8, 9, 10, 11, 14, 15, 23, 25, 45, 47 *BETA*
Low Criticality	27, 34, 43 *CHI*	1, 3, 6, 17, 21, 28, 29, 30, 31, 32, 33, 35, 36, 37, 38, 39, 41, 46, 49, 50, 51, 52, 53, 54 *DELTA*

Note:
- Only strategies scoring an average rating of "easily accomplished" are placed in the high feasibility category.
- Strategies ranked in the top fifty-percent of the criticality ranking are placed in the high criticality category.

Note: See Appendix C for the complete Round Two Instrument with Feasibility Ratings. See Table 2 for details on each strategy.

Now that a system is in place to prioritize the strategies, the stated barriers to implementation by the expert panel along with any stated strengths and weaknesses must be attached to each strategy. Tables 7,8,9, and 10 provide a listing of the fifty-four strategies with priority level, barriers to implementation, and strengths and weaknesses of each strategy.

Table 7 shows the fourteen strategies that fell into the Alpha level of priority. According to the expert panel, these are the most critical strategies that are easily accomplished. These are the strategies that should first be considered by the tourism industry. Being redundant in stressing the point, these strategies will be the easiest to implement while being of the most critical nature toward reducing the propensity of terror attack.

Strategy 2 ranked the highest priority over all others. It addresses the subject of training first responders on how to minimize the effects of a terrorist attack. Otherwise, the Alpha level is heavily weighted with seven different strategies pertaining to sharing of information and on-premises security activities. A total of twelve strategies are listed at the Alpha level.

Table 7

Alpha Level Strategies with Barriers by Priority Level

(Alpha = High Criticality, High Feasibility)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Alpha	2	Additional training provided to teach first responders about terrorist goals and their role in limiting the success of a terrorist attack (i.e. what to do after the scene is stabilized).	▪ Consistency of quality of training. ▪ A decentralized law enforcement apparatus.	▪ Provides a sense of responsibility and involvement in the war on terror. ▪ First step toward educating the entire population on awareness.	▪ Takes time to accomplish. ▪ Skill deterioration due to infrequent training.
Alpha	12	Network with other communities to determine what programs have bee successful in combating terrorism.	▪ Incompatible technological systems	▪ Information sharing is critical in preventing an attack.	▪ Reluctance to share ideas that could be profitable. ▪ Determining success of programs if attacks are rare in the area.

Table 7 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Alpha	13	Implement a crisis management plan. Conduct threat assessments for special events and structures to include integrated response plans involving private and public first responders.	▪ Cost to meet demands of planning (equipment, personnel, etc.)	▪ Good deterrent.	▪ Different methods to conduct assessments. ▪ Cannot plan for everything.
Alpha	16	Conduct thorough background and credit checks on each employee.	▪ ACLU ▪ Position Dependant. ▪ Added expense.	▪ Reduces opportunity for terrorist infiltration into workforce.	▪ Time consuming. ▪ Could be circumvented.
Alpha	18	All employees should have identifying badges and/or tags.	▪ Expense of system.	▪ System provides positive identification of personnel. ▪ Additional layer of security that must be penetrated.	▪ Counterfeit badges can be obtained. ▪ ID badges can be lost or stolen. ▪ Complacency of security personnel in checking ID's.

Table 7 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Alpha	19	All working contractors should be provided with a contractor's Id tag or badge.	▪ Expense of system. ▪ (Same as strategy 18).	▪ System provides positive identification of personnel. ▪ Additional layer of security that must be penetrated.	▪ Counterfeit badges can be obtained. ▪ ID badges can be lost or stolen. ▪ Complacency of security personnel in checking ID's.
Alpha	20	All employees should come through security check point and verified that they are an active employee.	▪ Additional personnel and equipment. ▪ Issuing of policy and procedures.	▪ Good preventative measures.	▪ Employees may circumvent the system due to inconvenience. ▪ Complacency at checkpoint.
Alpha	22	Frequent and high profile public service announcements regarding suspicious activities in or near venue, i.e. patrons should maintain control of their belongings.		▪ Keeps public aware.	▪ Guests may become complacent after hearing repetitive announcements. ▪ Terrorists hear the announcements as well.

Table 7 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Alpha	24	Deploy plainclothes law enforcement personnel to detect and obtain critical information from within the crowds. Personnel can be used for intelligence gathering and counter surveillance engagement.	▪ Cost associated with additional personnel.	▪ Can obtain information not found by other means. ▪ Can detect preplanning surveillance by terrorists.	
Alpha	26	Increase cooperative effort/ commitment with federal, state and municipal entities.	▪ Territorial issues.	▪ Increases effectiveness.	▪ Rotating administrations cannot mandate cooperation.
Alpha	40	Use of trained dogs to detect weapons/ contraband. Deploy K9 units to assist in bomb detection.	▪ Expensive. ▪ Fear of possible litigation.	▪ One of the most effective available deterrents.	
Alpha	42	Recognize you (tourism venue) are a target.		▪ Increase organizational awareness.	

Table 7 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Alpha	44	Have regularly scheduled meetings with area venues to keep them informed of changing trends in security and to allow them a voice to express their concerns.	▪ Trust issues between entities.		
Alpha	48	Utilize off-hour perimeter security patrols at gates and fences. All outer perimeters should be patrolled on a regular unscheduled time span.			

The Beta level in Table 8 shows a total of thirteen strategies falling into the second highest priority level. Six of these thirteen strategies are focused on sharing of information and networking, a strong point brought forth in the work of Calhoun and Weston's proposal on contemporary threat management. Considering a similar emphasis in the Alpha level, it shows the importance that the expert panel places on communication within and outside the tourism sector. This is supported by the WTTC action plan and DHS recommendations discussed in previous sections.

To distinguish between the Alpha and Beta levels, it is important to note that all the strategies are in the top fifty percent regarding criticality. The difference is in the feasibility when considering implementation. Only Alpha strategies were rated as being easily accomplished. At the Beta level, twelve of the thirteen strategies were reated as feasible. Only one, strategy 11, received a rating less then feasible. It was the high criticality value that kept strategy 11 at the Beta level of priority. Strategy 11 deals with the cooperation of the news media.

It can also be noted here that the study yielded four strategies that in some form addressed planning and risk assessment. Of those four strategies, three fell into the top fifty percent regarding criticality. Strategies 13 and 42 are in the Alpha level of priority and Strategy 8 fell into the Beta level. Sound security plans, re-assessment, and planning adjustments are all discussed in the WTTC and DHS recommendations.

Table 8

Beta Level Strategies with Barriers by Priority Level

(Beta = High Criticality, Lo Feasibility)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Beta	4	Publicize as many events as possible as being multi-national. Tourism must be advertised for success. Use of in-place marketing systems to stress diversity will create additional considerations for terrorist in planning an attack.		▪ Cost effective.	▪ Terrorists do not care who they harm with regards to ethnicity or religion. ▪ Minority groups may feel used and create distrust.
Beta	5	Train event and safety specialists in dynamic as opposed to static security techniques. Utilize diverse and randomized methods for screening tourists upon entry to an event and for controlling crowd flow during an event. Where warranted bag, purse, and package checks of guests, participants, invitees, and employees.	▪ Inconvenience. ▪ 4th amendment issues. ▪ Racial profiling issues. ▪ Limited personnel resources. ▪ Cost.	▪ Good deterrent.	▪ Lack of consistency by low paid personnel.

Table 8 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Beta	7	Improve physical design of facilities to take into account the terrorist threat. Design new facilities with crime prevention in mind. Remodel existing facilities with crime prevention in mind.	▪ Increased cost of design	▪ Effective in providing protection and proven deterrent.	▪ Education of architects in CPTED.
Beta	8	Have a unified method to determine risks.	▪ Personnel resistance to change or methods not of their own.	▪ Standardization.	▪ If terrorists obtain "the standard" it can become a weakness or exploited.
Beta	9	Reach out to the community for intelligence. Establish communication between hotels, parks, and other events with local and federal law enforcement.	▪ Requires cooperation among many different interest groups.	▪ "Grass roots" idea. ▪ Cost effective.	▪ Some may resist participation for fear of reprisal. ▪ Some information may be overlooked due to high volume. ▪ Reluctance of law enforcement to involve outside entities.

Table 8 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Beta	10	Having community leaders, including religious leaders, speak out in a unified voice against terrorism since most recent acts of terrorism are based on some slanted view of religion.	▪ Extremists have distorted view of their religion.	▪ May affect a minute portion of religious fanatics who believe terrorists. ▪ Cost effective.	▪ Terrorists not likely to consider views of conservative religious leaders. ▪ Islamic religious leaders not likely to speak out against own religious radicals.
Beta	11	Ask the media's cooperation in correctly portraying these people. They are not suicide bombers, but homicide bombers, they are not freedom fighters, but murderers, and they are not to be admired, but scorned.	▪ Lack of support from liberal media.		▪ Bias media will report what/ how benefits ratings or pushes an agenda.

Table 8 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Beta	14	Improve intelligence gathering, analysis, and sharing capabilities among private and public security professionals.	▪ Cost; time consuming; security clearances; need to know basis of personnel.	▪ Information sharing is critical in preventing an attack.	▪ Unwanted or misdirected dissemination. Terrorists can infiltrate both entities. Security breaches are possible. Information overload.
Beta	15	Where applicable, personal screening of guests, participates, invitees, and employees should be conducted.	▪ Inconvenience to public. ▪ Crowd control. ▪ Racial profiling issues. ▪ Could cause uproar among privacy advocates.	▪ Good deterrent.	▪ Terrorists can plan around or circumvent. ▪ Consistency of training and complacency.

Table 8 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Beta	23	Implement the utilization of closed circuit television in tourist areas at venue and core surrounding area.	▪ Cost. ▪ Additional equipment and personnel to operate.	▪ Good deterrent and surveillance method.	
Beta	25	Utilize special security units that provide confidence to visitors (Examples: Bike patrols, Mounted Units, Motorcycle Units).	▪ Cost beyond basic services.	▪ Public relations tool.	▪ Not cost effective.
Beta	45	Local law enforcement should become involved in organizations and serve on boards when appropriate or when asked to do so; i.e. hotel and lodging associations, convention and visitors bureaus, chamber of commerce, etc.	▪ Time consuming for job function.		

Table 8 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Beta	47	Cross communicate with local and fed law enforcement on updated terrorist intelligence.	▪ Reoccurring changes in administrations can alter cooperation levels.	▪ Front line defense mechanisms become more effective.	▪ Information overload can result.

Moving into the Chi level of priority, there were only three strategies as can be seen in Table 9. The Chi level contains strategies that are in the lower fifty percentile of criticality, however they are easily accomplished. The three strategies in the Chi level pertained to the training of employees on security issues and securing personnel access to a facility. Looking at the barriers and weaknesses to the strategies, there is a concern about the lower wage earning employees. These type workers are generally viewed as not taking the training seriously and not staying on the job for an extended period of time. A high turn over rate of employment would cause a high level of repetitive training with new employees on a continual basis.

Delta level priority indicates strategies that are low in criticality and not feasible to implement. These are strategies to which a venue operator would give the least amount of consideration. Twenty-four proposed strategies fell into this level of priority as shown in Table 10. The strategy topics covered the gamut, however, a cluster of six strategies were related to the use of technology. In fact, all the strategies developed in this study involving the use of technology fell into the Delta level. The common barrier to implementation that ultimately led to being placed at the Delta level is cost. This should be monitored closely as technology continues to advance and costs decrease. Federal funding might be considered to offset costs.

Table 9

Chi Level Strategies with Barriers by Priority Level

(Chi = Lo Criticality, High Feasibility)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Chi	27	Train personnel (both police and private sector) in recognizing potential threats and actions that warrant police intervention A training program that empowers every employee to be a security agent.	▪ Employees must take training serious. ▪ Repetitive training where high turnover exists.	▪ Vital to educate employees.	▪ Reluctance of low wage earners to take training seriously. ▪ Lack of transfer and continuous training.
Chi	34	High visibility of law enforcement personnel for a deterrent aspect.	▪ Costs.	▪ Deterrent aspect. ▪ Immediate availability of personnel.	▪ Training adequate numbers of personnel.
Chi	43	Tighten-up security at loading dock operations at large venues. Only allow access to those on check lists. Implement standard operating procedures for delivery. Any and all delivery vehicles should be recorded and driver's license should be recorded.			

Table 10

Delta Level Strategies with Barriers by Priority Level

(Delta = Lo Criticality, Lo Feasibility)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	1	Terrorism only works due to media. National government needs to have agreements with media regarding a terrorist attack; much the same way they control war footage.	▪ Unconstitutional. ▪ Gaining cooperation of media.	▪ Media coverage gives terrorists the publicity they desire, cutting them off reduces the rewards of the risk.	▪ Freedom of speech violation.
Delta	3	Make non-vital targets more readily available in order to channel terrorist activity to those locations. Ensure non-vital targets are politically acceptable.	▪ Lack of political support. ▪ Public outcries for stating certain targets are acceptable. ▪ Legal/ ethical issues.	▪ Exercising limited control over terrorists.	▪ These type targets not of interest to terrorist.

Table 10 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	6	Design increasing layers of security around an event based upon a risk assessment. In line with dynamic techniques, make heavy use of a double entrance approach; it will be difficult for terrorists to breach if they are unsure what measures will be in place after the initial entrance. Any persons attempting to leave after the first entrance and before the second entrance would be considered suspect.	▪ Cost of additional manpower.	▪ Common sense approach. ▪ Reduces chance of terrorist's success.	▪ Terrorists will probe security layers to find weaknesses.
Delta	17	Outside contractors for the event or location should have backgrounds conducted on own employees by third party.	▪ Relying on contractors to ensure employees are legitimate. ▪ Added expense to contractor is passed on to customer.	▪ Diminishes opportunity for terrorists to access vulnerable areas.	▪ Temptation of contractor falsify background check to reduce costs.

Table 10 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	21	All contractors should have a specific parking area and be subject to vehicle screening by security personnel.	▪ Availability of space.	▪ Good deterrent.	
Delta	28	Train, equip, and staff police personnel with CBRNE gear.	▪ Cost.	▪ Protection of responders.	▪ Availability of gear when needed.
Delta	29	Target-harden venues to include metal detectors.	▪ Cost. ▪ Logistics.		▪ Complacency of personnel. ▪ False sense of security.
Delta	30	Stage specially trained law enforcement personnel for bomb intervention near the venue. Train staff and deploy personnel in bomb detection/suppression. Deploy mechanical bomb detection devices with police and private sector security staff.	▪ Expensive.		▪ Only feasible in large metropolitan areas.

Table 10 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	31	Fund, budget, and deploy air unit support to monitor event.	▪ Very expensive.	▪ Provides observation platform.	▪ Becoming overly dependant on a system is not available 100% (bad weather).
Delta	32	Billboards with instructions on what to do if a crisis occurs. People should always know where they are and where they are going or where they need to go.		▪ Keeps security on the minds of public. ▪ Cost effective.	▪ Makes terrorists aware of evacuation plans and could use to deploy secondary bombs.
Delta	35	Enhance security procedures to include the use of manual and electronic search methods.			
Delta	36	Utilize citizen patrols that have been specifically trained to enhance security or law enforcement.	▪ Maintaining level of training.	▪ Cost effective.	▪ Can be difficult to train.

Table 10 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	37	Plan with the local police department.	▪ Dependent upon specific event.		
Delta	38	Ask your guests to be aware. Don't scare them. Tell them their stay will be more enjoyable if they are aware of their surroundings and take simple precautions to keep them and their belongings safe.		▪ Increases public awareness.	▪ Hard to determine effectiveness of strategy. ▪ May increase false reports.
Delta	39	Partner with the media to publish safety tips and location maps.	▪ May or may not be without costs.		▪ No assurance on number of people who will be receptive.
Delta	41	Use training drills to prevent skill decay. Train and retrain.	▪ Available time for training.		

Table 10 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	46	Use barricades to prevent vehicular intrusion. Employ concrete barriers and spike strips. Keep vehicles at a distance from the perimeter.	▪ Cost.	▪ These are proven methods.	▪ Can create time delays at large venues.
Delta	49	Provide ongoing training for security personnel on terrorists' activity and tactics.	▪ Cost.		▪ Lack of transfer.
Delta	50	Employ cameras with a big screen picture of people walking in and around specific strategic areas of interest. Similar to radar trailers; "Do you see how fast you are driving?"	▪ Costs.		▪ Easily negotiated by terrorists.
Delta	51	Use photo identification and personalized security devices (i.e. ID cards, bracelets, etc.) for patrons.	▪ Cost. ▪ Providing the ID to the patron creates time delay issues.	▪ Good deterrent.	

Table 10 (continued)

Priority Level	Strategy Number	Strategy	Stated Barriers to Implementation	Strengths	Weaknesses
Delta	52	Install motion detectors that are voice activated and state something to the effect that the premise is under law enforcement surveillance.	▪ Cost.		▪ Small effect/ return.
Delta	53	Require advanced reservations to access vital places. Scan cards are mailed to allow access to the event.	▪ Cost. ▪ Time constraints for reservations.		
Delta	54	Use radioactive material detection devices throughout facilities or event areas.	▪ Expensive.	▪ Quick screening technique.	

During the analysis of priority levels, the researcher began to recognize similar generalized topics among strategies. Sorting the strategies into subordinate categories was based on the researcher's eighteen years experience in law enforcement and training development. The entire data collection from this study is included and can be used by future researchers to come to their own conclusions about similarities or subcategories of the strategies.

Looking at the subordinate category of Training for example, there are five strategies involving some form of training needs, Strategy number 2 at the Alpha Level, Strategy Number 5 at the Beta Level, Strategy Number 27 at the Chi Level, and Strategies Number 41 and 49 at the Delta Level. Yet the details on the type of training are of a different nature. Strategy Number 2 involves training first responders on their role in circumventing the success of terrorists following an attack. Strategy Number 5 states a need to train event personnel in dynamic security techniques. Strategy Number 27 explains the need to train personnel in recognizing behaviors that warrant police and security intervention prelude to an attack. Strategy Number 41 promotes scenario training on an ongoing basis to prevent personnel skill decay. And finally, Strategy Number 49 involves educating personnel on terrorists' tactics and methods. Again, all afore mentioned strategies involve training in various forms and each training strategy has been prioritized for the user who is looking for training solutions.

The subordinate category of Communication/ Liaison deals with a myriad of entities including the general public. Twelve strategies within this subordinate category range from marketing techniques to the sharing of information between law enforcement, private security, and the community. Planning/ Assessment strategies involve risk and

crisis management issues as well as organizations making the connection with being a target for attack. Different Background Check strategies emerged as a subcategory as an obvious to means reduce infiltration of terrorists into the workforce or other related work forces. Strategies within the ID Badge/ Security Entrance deal with not only employee issues, but also the attendees of various events or locations. There are various strategies involving Specialty Security Units that form a subcategory and range from technical expertise to simple public relations. Architectural Design is a subcategory that appeared because of six different strategies that stated the need for various types of functional designs for physical protection to include new construction and remodeling of existing venues. Gaining the cooperation of the media was recognized as a subordinate category with three different strategies being proposed. And finally the last subordinate category was Technology Based strategies of which there were six.

The emergent subordinate categories are Training, Communication/ Liaison, Planning/ Assessment, Background Checks, Identification Badges/ Secure Entrance, Specialized Security Units, Architectural Design, Media Cooperation, and Technology Based. Each one of these subordinate categories came to light because of similarities between strategies even though each strategy was a stand-alone solution or need.

Placing strategies in subordinate categories will help the venue operator to see what areas his or her organization would most benefit. So now, what emerges in the form of a prototype guideline is a reference format where specific strategies can be broken down into four levels of priority and within each level the strategies can be placed into nine different subordinate categories as shown in Table 11.

To summarize the use of the Prototype Guidelines, the user will have at first glance four priority levels to consider. Within each level the user can quickly discern among nine different areas or types of strategies from which address their individual needs. Or, the user may have an issue regarding Planning and Assessment. In that case, the user can look to the appropriate subordinate category and have a list of strategies provided in a prioritized format. Once a particular area is selected, the user can refer to the detailed list of strategies with additional support from comments stating the barriers to implementation, the strengths and the weaknesses of each strategy as was shown in Tables 7, 8, 9, and 10.

Table 11

Prototype Guidelines

Alpha level strategies in subordinate categories

Training	Communication/ Liaison	Planning/ Assessment	Background Checks	ID Badges/ Secure Entrance	Specialty Security Units	Architectural Design	Media Cooperation	Technology Based
2	12,22,26,44	13,42	16	18,19,20	24,40,48			

Beta level strategies in subordinate categories

Training	Communication/ Liaison	Planning/ Assessment	Background Checks	ID Badges/ Secure Entrance	Specialty Security Units	Architectural Design	Media Cooperation	Technology Based
5	4,9,10,14,45,47	8		15	25	7,23	11	

Chi level strategies in subordinate categories

Training	Communication/ Liaison	Planning/ Assessment	Background Checks	ID Badges/ Secure Entrance	Specialty Security Units	Architectural Design	Media Cooperation	Technology Based
27				43	34			

Delta level strategies in subordinate categories

Training	Communication/ Liaison	Planning/ Assessment	Background Checks	ID Badges/ Secure Entrance	Specialty Security Units	Architectural Design	Media Cooperation	Technology Based
41,49	32,38	37	17	21,51,53	30,31,36	3,6,29,46	1,39	28,33,35,50, 52,54

Note: See appendix A for details on each strategy.

Ancillary Findings

There are several findings not anticipated by the researcher, but worthy of being noted in this section. Continuing to consider the subordinate categories, Communications/ Liaison stands out from the other eight in that it contains more strategies than any other subordinate category. And of its twelve strategies, ten fell into the high criticality ranking. Four of the strategies are at the Alpha Level meaning they are of high criticality and are easily accomplished when implemented. This is an indication that among the subject matter experts, communications and liaison strategies are of the greatest importance in combating the threat of terror attack in the tourism industry. The two remaining strategies fell into the Delta Level. Strategy 32 proposed the use of billboards to instruct patrons what to do and where to go if an attack should occur. The weakness to this strategy is that the terrorist can use this information to plan their attack. For example, secondary bombs can be placed along escape routes or other areas where crowds will likely congregate. Strategy 38 expresses a need to ask guests to help with some security aspects. Weaknesses for this strategy were listed as difficulty to determine effectiveness and the likelihood of false reports. The stated weaknesses of these strategies are evidence as to the reason for them receiving a low priority level.

The subordinate category receiving the second highest number of strategies was Specialty Security Units. It received eight proposed strategies of which only three fell into the Alpha Level and one fell into the Beta Level. No other subordinate categories drew more than six strategies.

The subordinate category of Background Checks contains two strategies. Strategy 16 deals with background checks done on employees of the venue and was rated at the

Alpha Level. Strategy 17 deals with background checks done by independent contractors on their own employees prior to them being given access to the venue, however this strategy received a rating at the Delta Level. A clue as to the reason for the disparity between the two strategies is found in the comments made by the expert panel. Strategy 17 is viewed as having barriers and weaknesses by relying on the contractor to perform adequate background checks on employees due to added costs for the contractor.

Strategy 11 is a point of interest in that it is the only strategy to receive a high criticality ranking along side a feasibility rating of not being feasible. All other critical strategies were rated at "easily accomplished" or "feasible." Strategy 11 states the need to have cooperation with the media in portraying terrorists as murders and not freedom fighters or suicide bombers. The contention is that the media is recognized as a tool of the terrorists and reducing the affect of media coverage would weaken the terrorists. This is of course a hotbed of political debate among those more apt to be outside the realm of academic research and more likely to be among those who debate political strategy or correctness issues.

Another unexpected finding is within the Technology Based subordinate category. All of the strategies were clustered in the Delta Level. There are six strategies in all dealing with technologies such as gear to protect against chemical biological and nuclear exposure, software, automated cameras, electronic search equipment, and radioactive material detection equipment. The common barrier to implementation among these strategies is cost. These strategies also all ranked low on criticality among subject matter experts.

Finally, the researcher noticed areas for comparison between some of the strategies formulated in this study and the work done by Calhoun and Weston (2003). In Calhoun and Weston's work on threat management, they propose a process by which organizations can identify, investigate, and manage people who may be a threat to physically harm other people within the workplace (p. 1). When establishing a threat management process, they posit specific criteria that must be in place for its development. The various strategies and subordinate categories that have culminated from this study have profound similarities to their recommended criteria.

The first task in Calhoun and Weston's (2003) contemporary threat management process is to train employees in what to look for and how to respond. The subordinate category of Training contains specific strategies that deal with the very same issues. Furthermore, Calhoun and Weston recommend reaching to other areas and organizations and developing lines of communication so that information and experiences can be shared (p.264). The subordinate category Communications/ Liaison has been pointed out earlier to hold the highest importance among the subject matter experts. In this study, the greatest need to reduce the chance of terror attack in the tourism industry is in strategies involving information sharing and communication among agencies, jurisdictions, businesses, and communities as evidenced by the largest number of strategies than any other subordinate category in this study.

When Calhoun and Weston refer to anyone who is the subject of threats of violence, they refer to them as a target (p. 275). One of the most profound yet simple strategies developed during this study is Strategy 42. Ranked in the Alpha Level, it states, "Recognize you are a target." This is crucial in any organization before attempting to

develop a crisis management plan. Along those same lines, Calhoun and Weston recommend portraying a protective image to the target. This means keeping them informed, provide instructions, and maintaining a calm atmosphere (p. 275). Not only does that involve communication to patrons through the use of signs and public announcements, but also by creating a visual image; appearing safe and vigilant with the use of specialized units employed at the venue. A list of strategies to address this is found in the subordinate category Specialty Security Units.

Summary of Results

The subject matter expert panel was instructed to suggest, refine, and prioritize strategies that can be used by the tourism industry to reduce the propensity for terror attack. The Delphi study resulted in fifty-four strategies. To best describe the results, the expert panel ranked these strategies as to criticality and rated the strategies as to feasibility to implementation. Using that data, the strategies were inserted into a criticality-feasibility matrix. Each quadrant of the matrix was then labeled as to its priority level. Then, the researcher was able to cluster individual strategies into subordinate categories, nine in total. The expert panel also provided comments on each strategy regarding its strengths, weaknesses, and any barriers to implementation. Thus in answer to the fourth research question, “What are the prototype guidelines to apply the solutions to the stated needs?” the final format presents the strategies listed by subordinate category in priority level and supported by subject matter expert comments regarding implementation.

CHAPTER V

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary

Since the events of September 11, 2001, the tourism industry in the United States has come to realize the threat of terror attack within this country's borders must be considered plausible. Yet, there is no set of guidelines to which the tourism industry can refer for assistance in devising strategies that may be common areas of concern among the various tourism sectors.

This study identified the strategies that can reduce the propensity of terror attack directed at tourism venues. These strategies were prioritized and placed into a format that describes potential impact and consequences to implementation to tourism risk management policy makers. It expanded on the limited amount of research base to security officials and experts in the tourism field by correlating views and opinions of experts regarding terrorism risk management as to what are the important issues regarding tourism security. The results are a list of strategies with assessment to criticality and feasibility.

This study addressed the following the questions:

1. What are the needs of the Tourism Industry to reduce the risk of terrorist attack?
2. What are the solutions to the stated needs?
3. What are the barriers to the stated solutions?
4. What are the prototype guidelines to apply the solutions to the stated needs?

This study followed the Delphi technique using three rounds of questionnaires distributed to an expert panel via electronic mail thus providing structure for the group

process. The Delphi technique thwarts the barrier of financial and time constraints associated with travel and allow geographically dispersed subject matter experts to participate from their respective locations (Linstone & Turoff, 1979).

A core group of subject matter experts was gathered through a literature search, professional organization listings, and professional conference rosters. The sample consisted of subject matter experts who matched the definition of an individual who has both academic and applied knowledge in the tourism security field. Those in the core group were contacted and asked to nominate peers they believe to fit the criteria. This resulted in a list of seventy-six experts including the original twelve from the core group. Twenty-four experts completed the round one questionnaire, twelve successfully completed round two and twelve participants successfully completed the round three questionnaires.

Seventy-six tourism security experts were invited to participate in the study and were sent invitation via email on April 19, 2004. The first round questionnaire provided an open-ended question seeking opinions from the expert panel. The responses from all respondents were compiled into a comprehensive list of strategies that the experts proposed to reduce the propensity for terror attacks in the tourism industry. The complete list of ideas from the first round was distributed in a second round questionnaire to the expert panel. The panel was asked to further clarify each idea discussing its strengths and weaknesses and to rate the feasibility of each item and to state any barriers to implementing the particular strategy. The third round asked the expert panel to rank the list of strategies from most critical to the least critical in regards to the effect that the

strategy will have in decreasing the chance of a terrorist attack. The study was completed on February 10, 2005.

The first research question addressed in this study was "What are the needs of the tourism industry to reduce the risk of terrorist attack?" The first round questionnaire asked the panel of experts "What actions can be taken at events and locations (hotels, resorts, theme parks, convention centers, public gatherings, etc.) frequented by tourists that could reduce the propensity for terror attacks?" The result was a comprehensive list of fifty-four strategies.

The second research question to be addressed was "What are the solutions to the stated needs?" The second round questionnaire, which included the comprehensive list of fifty-four strategies, was distributed to expert panel. The panel was asked to review the list and provide for each strategy its strengths and weaknesses, a rating of its feasibility to implementation, and finally any barriers to implementation. From this data, an average rating value for feasibility was calculated and implanted in the criticality-feasibility matrix.

The third research question to be addressed was "What are the barriers to the stated solutions?" The descriptive data provided in the second round questionnaire on barriers to implementing each strategy was analyzed. A format for considering strategy implementation began to emerge.

In the final round, the expert panel was asked to rank the list of strategies from the most critical to the least critical. The average rank order for criticality of each strategy was calculated. This rank data was then used in conjunction with the feasibility rating data to complete the matrix, which clustered strategies according to their criticality

ranking and feasibility rating. Each quadrant of the matrix was assigned a level designated by Alpha, Beta, Chi, and Delta. Alpha level strategies are known to be of the highest criticality and the highest degree of feasibility, Beta level strategies are highly critical, but have a low degree of feasibility for implementation, the Chi level strategies are designated as having low criticality and are easily implemented, and finally, Delta level strategies are of a low critical nature and difficult to implement.

Combining the priority levels with the stated barriers to implementation identified by the expert panel along with any stated strengths and weaknesses comprises the prototype guidelines that address the fourth research question of "What are the prototype guidelines to apply the solutions to the stated needs?"

When working toward policy decisions, the objectives of a Delphi are a combination of discovering all possible options for consideration, estimates of impact and consequences of each option, and determine acceptability of any option. The overall goal is not one of creating consensus as much as it is to expose all ideas and strategies and the pro and con arguments for each (Linstone & Turoff, 1979). A list of fifty-four strategies was developed by this study. Experts who gave opinions on strengths and weakness, acceptability, and its critical nature examined each strategy.

Conclusions

The data produced as a result of this descriptive study has led the researcher to the following conclusions.

1. Strategy Number 2 received the highest criticality ranking over all other strategies and therefore should be highly considered by the tourism industry. It involves

training first responders on their role in circumventing the success of terrorists following an attack.

2. The subordinate category Communication/ Liaison contains the largest number of strategies indicating the significance of this category among experts. Of the twelve strategies within this subordinate category, ten were ranked as highly critical. No other subordinate category received this high number of strategies.

3. The subordinate category to contain the second highest number of strategies is that of Specialty Security Units again indicating the importance of the topic among experts. Half of the eight strategies were ranked as highly critical.

4. All six strategies of the Technology Based subordinate category fell into the Delta level of priority, which is the lowest priority level showing that at this point, the experts do not believe that technology is the best tool to protect against terrorism in the tourism industry. The common theme among these strategies is the cost barrier. Finding ways to fund advanced technologies in order to make them more feasible to implement will be a challenge, however, the trade off in increased safety can justify the cost.

5. Three strategies emerged in the Media Cooperation subordinate category demonstrating that the media is viewed as tool of the terrorist. Though controlling the media could be effective, the expert panel was quick to point out that due to its unconstitutionality, it is not feasible. Among the twenty-five strategies ranked as highly critical, Strategy 11 was the only strategy to receive a feasibility rating of “not feasible.” This topic opens the door to a lengthy political debate.

6. Two Background Check strategies emerged as a subcategory, however Strategy 16 involving backgrounds done on venue employees fell into the Alpha priority level

while Strategy 17 involving background checks done on contractors fell into the Delta priority level indicating the concern among experts that the contractors would fail to provide adequate background investigation practices in order to save on the additional overhead cost. This is an opportunity for either the private or public sector to standardize backgrounds and research the most effective and efficient methods to conduct background checks for security purposes. An accreditation process or entity could serve to streamline appropriate background practices which reduce time and cost.

7. The six different strategies that appeared in the Architectural Design subordinate category expresses the experts' opinion of the need for various types of functional designs for physical protection to include new construction and remodeling of existing venues. Crime Prevention Through Environmental Design or CPTED has been expressed by the law enforcement community for many years, yet training in this area at the academic and professional levels seems slow to follow. Designing a facility around security systems would be a much more effective method than installing security systems after the fact. Even more expensive is the remodeling of a venue when a safety concern arises after completion of the facility.

8. During the study, some SME's who were invited to participate wanted recognition for their company while others declined to participate because they did not wish to divulge information or technologies that they regarded as trade secrets from which they stood to profit. This is indicative of communication roadblocks afflicting this industry.

Recommendations

The data discovered in this study are descriptive and should primarily be used as a reference during decision making by those operating in the tourism industry. As a result of this study, the following recommendations are presented.

Recommendations Based on the Study

1. The guidelines developed in this study should be used by operators of tourism venues to make the best use of limited resources.

2. National or international conferences should be established to further discuss these issues to include governmental entities such as the Homeland Security, Department of Defense, and F.B.I. as well as private sector organizations.

3. A greater number of communications mediums should be established to facilitate the exchange of ideas and experiences between affected professionals. This could also be extended to vendors to allow secure cross communication whereby presentation of available technologies could be accomplished more expediently and at a reduced cost. An example would be a secure web net where presentations could be made without threat of infiltration.

4. Insurance providers should use this information to establish validated guidelines so that if prospective clients adhered to the recommendations a reduction in premiums could be offered.

5. Training should be implemented at the academic and professional levels for architects regarding facility designs that incorporate security features to guard against terror attack. Designs from the ground up can also incorporate the aesthetic qualities desired by the customer. Expenditures for new facilities with security design features

will be more cost effective than having to remodel at a later time after weaknesses are discovered.

6. Table top exercises or scenario training that may be conducted by law enforcement entities should be expanded to include other affected organizations such as hotel operators, convention centers, private security forces, and other tourism related businesses.

7. Other entities may benefit from this study, such as public school systems, the energy production industry, hospital systems, and pipeline systems should consider the information from this study. There are more that could benefit from this study and only a few have been listed.

Recommendations for Future Study

1. Regarding the Technology Based subordinate category, a study should be conducted involving only technological strategies. Though viewed in this study as mostly cost prohibitive, technology is a rapidly changing arena and in the future cost may be overcome as a barrier as the technologies improve.

2. Over time, strategies, technologies, and tactics can change. In order to stay abreast of a fluid environment, this study should be replicated or at least similar studies conducted so as to maintain updated information for the affected professionals.

3. A more accessible validated background check system should be developed for contractors to be able to provide safe employees to customers in a cost effective manner.

4. A predetermined list of strategies in future studies would speed up the process and possibly increase the number of participants. Furthermore, a computer based study

with a multiple choice answer system that reduces the amount of time to participate may entice a larger pool of participants.

5. Studies directed at determining the best environmental design practices regarding safety could be beneficial in many sectors within and outside the tourism industry.

6. In future research, a close look should be taken as to developing better methods to rate feasibility of the strategies.

7. An effort should be made to determine what can be done to make critical strategies more feasible for a larger cross section of the tourism industry.

8. Data collection from interrogation of terrorists to determine if any factors exist that cause a change in plans are target selection. If factors do exist, then strategies could be developed around that information.

These recommendations are presented so that future studies can develop additional data from which to test the validity of these suggestions.

REFERENCES

Adler, M., & Ziglio, E. (1996). *Gazing into the oracle: The Delphi method and its application to social policy and public health.* London: Kingsley Publishers.

Alexander, Y. (2002). *Combating terrorism.* Ann Arbor: The University of Michigan Press.

Bali Bomb Plotter Trial Starts. (2003). Retrieved July 27, 2003, from *http://www.cbsnews.com/stories/2003/05/12/attack/printable553470.shtml.*

Bali Bomb Lawyers Seek to Move Trial. (2003). Retrieved January 07, 2003, from *http://cnn.worldnews.printhis.clickability.com/pt/cpt?action.*

Cain, Sandi. (January, 2002). Tourism officials focus on security of events and sites as key to attracting visitors. Retrieved November 28, 2004, from *http://www.hotel-online.com/news/pr2002_1st/Jan02_Security.html*

Calhoun, F. & Weston, S. (2003). *Contemporary threat management.* San Diego: Specialized Training Services Company.

Crockford, N. (1980). *An introduction to risk management.* Cambridge, Great Britain: Woodhead-Faulkner Limited.

Department of Homeland Security. (2003). *The physical protection of critical infrastructures and key assets.* Washington, DC: U.S. Government Printing Office.

Dershowitz, A. M. (2002). *Why terrorism works.* New Haven, CT: R.R. Donnelley & Sons Co., Inc.

Essner, J. (2003). Terrorism's impact on tourism: What the industry may learn from Egypt's struggle with al-gama's al-islamiya. Retrieved from *http://sand.miis.edu/ research/student_ research/Essner_Tourist%20Terrorism.pdf.*

Gilmore, G.D. & Campbell, M.D. (2004). *Needs and capacity assessment strategies for health promotion and health education.* Boston: Jones and Bartlett Publishers.

Glendon, A., McKenna, E. (1995). *Human safety and risk management.* London: Chapman & Hall.

Gold, M. & Holland, M. (October 17, 2003). Bloodied but unbowed – tourism's battle with terrorism. Retrieved November 27, 2004, from *http://www.pkf.co.uk/web/PKFWebb.nsf*

Goss, A. (April 29, 2003). Futurist forecasts terrorism's continuing effects on tourism. Retrieved November 27, 2004, from *http://www.udel.edu/PR/Udaily/2003/cetron042903.html*

Hall, C.M. (1997). *Tourism and politics: Policy, power and place.* New York: John Wiley & Sons.

Isaac, S. & Michael, W.B. (1997). *Handbook in research and evaluation,*3rd Edition. San Diego: Educational and Industrial Testing Services.

LaMoshi, Gary. (September 19, 2003). Indonesia rethinks tourism, terrorism. Retrieved November 27, 2004, from *http://www.atimes.com/atimes/Southeast_Asia/EI9A02.html*

Linstone, H.A. & Turoff, M. (1979). *The delphi method, techniques and applications.* London: Addison-Wesley Publishing Co.

Marquardt, E. (March 19, 2003). Spanish elections reinforce terrorism as effective political weapon. Retrieved August 07, 2004, from *http://www.pinr.com/report.php*

Meltzer, M. (1983). *The terrorists.* New York: Harper & Row.

Muehsam, M. & Tarlow, P.E. (1996). *Tourism, crime, and international security issues.* Wilmington, DE: John Wiley & Sons.

National security and defense. (n.d.). Retrieved April 23, 2005, from *http://www.ncpa.org/pi/congress/cong9.html*

Netanyahu, B. (2001). *Fighting terrorism.* New York: Farrar, Straus and Giroux.

Online newshour transcript. (1997). Terrorist attack. Retrieved July 27, 2003, from *http://www.pbs.org/newshour/bb/middle_east/july-dec97/egypt_11-17.html.*

Pill, J., (1971). The Delphi method: Substance, context, a critique and an annotated bibliography. *Socio-Economic Planning Science. V, 57-71.*

Presser, S. & Saners, E. (1994). Survey prestesting; Do different methods produce different results? *Sociological Methodology.* 24, 73-104.

Safe Democracy Foundation, (March 9, 2005). Terrorism and the travel industry-international summit on democracy, terrorism and security. Retrieved February 3, 2006, from *http://english.safe-democracy.org/keynotes/terrorism-and-the-travel-industry.htm*l

Sonmez, S. (1997). Tourism, terrorism and crisis management. Paper presented at the meeting of War, Terrorism, Tourism, Dubrovnik, Croatia, "Institut za Turizm: International Conference.

Sonmez, S.F. & Tarlow, P.E. (1999). Tourism in crisis: Managing the effects of terrorism. *Journal of Travel Research,* 38(1), 13-19.

Tarlow, P.E. (2000). Conference reports – Las Vegas tourism security seminar. *Tourism Management,* 22, 205-212.

Tarlow, P.E. (2001a). Bridging the gaps – the ninth annual Las Vegas tourism security and safety conference. *International Journal of Tourism Research,* 3(3), 253-259.

Tarlow, P.E. (2001b). A site to see. *Security Management,* 48-53.

Tarlow, P.E. (2002). *Event risk management and safety.* New York: John Wiley & Sons.

Taylor, H., (May 14, 2003). Fear of increased travel risks inhibit vacation and travel plans. Retrieved February 3, 2006, from *http://www.harrisinteractive.com/harris_poll/printerfriend/index.asp?PID=377*

Travel & tourism security action plan. (2003). Retrieved November 28, 2003, from *http://wttc.org/frameset5.htm*

Turoff, M. (1970). The Policy Delphi. *Journal of Technological Forecasting and Social Change,* 2, 149-171.

Turoff, M. & Hiltz, S. (1996). Computer based Delphi processes. In M. Adler & E. Ziglio (Eds.), *Gazing into the oracle: The Delphi method and its application to social policy and public health.* London: Kingsley Publishers.

U.S. Department of State. (1992). *Patterns of global terrorism: 1991.* Washington, DC: Author.

U.S. troops capture terrorist behind cruise ship hijack. (2003). Retrieved June 23, 2003, from *http://www.straitstimes.asial.com/iraqwar/story/0,4395,183697,00.html.*

Weaver, W.T., (1971). The Delphi forecasting method. *Phi Delta Kappan,* LII, P.267-271.

Williams, P.E. (2000). Defining distance education roles and competencies for higher education institutions: A computer-mediated Delphi study. Department of

Educational Administration and Human Resource Development, Texas A&M University.

APPENDIX A

CORRESPONDENCE WITH PANEL

ROUND ONE

INVITATION EMAIL

Information Sheet

Development of Prototype Guidelines for Risk Management Against Terror Attack in the tourism Industry

You have been asked to participate in a research study being conducted at Texas A&M University regarding risk management in the tourism industry. You were selected to be a participant because of your past experience, expertise, and general interest in the area of tourism security. Your name was obtained through a literature search, professional organization listings, and professional conference rosters. The purpose of this study is to gather strategies and factors from tourism security professionals in order to formulate comments from which terrorism risk management policies can be developed. There shall be an attempt to correlate views and opinions regarding terrorism risk management and to allow respondents to react to and examine opposing viewpoints. The study shall put forth all possible options for consideration by individual, corporate, and agency policy makers. To provide further detail, an estimate of impact and consequences of any particular option as well as examination of the acceptability of any particular option shall be sought. The purpose of this study is NOT to make decisions for policy makers, but rather, to provide all available options presented by an informed group for consideration by policy makers.

The Delphi methodology is a widely used technique for the systematic development of expert opinion consensus. This methodology involves gathering data from a small group of persons who by professional reputation have been identified as "experts." If you agree to participate in this study, you will be asked to complete the following questionnaire as well as one or more subsequent questionnaires to be disseminated and returned via email, thus participating as a "panel expert." There shall be two or more questionnaires, but no more than four questionnaires in total. Each questionnaire should take approximately 25 to 30 minutes to complete. At the conclusion of the study, each participant shall receive a copy of the documented results.

This study is confidential and any link between the participant's identity and the data shall not be disclosed and destroyed at the conclusion of the study. No identifiers linking you to the study will be included in any sort of report that might be published.

By completing and returning this questionnaire, you agree to participate in this study. This research study has been reviewed b the Institutional Review Board – Human Subjects in Research, Texas A&M University. You may withdrawal from this study at any time without negative consequences to anyone or Texas A&M University. For research-related problems or questions regarding subjects' rights, you can contact the institutional Review board through Dr. Michael W. Buckley, director of Research Compliance, Office of Vice President for Research at (979) 845-8585 (mwbuckley@tamu.edu).

Sincerely,

Keith Smith
Research Associate

Clifford "Keith" Smith Department of Educational Administration and Human Development (979) 224-3342 : TexasAandM.PhDResearch@verizon.net	Dr. Walter F. Stenning, Committee Chair Department of Educational Administration and Human Development (979) 845-8380 wfs4666@tuxcom.net

ROUND ONE

FIRST REMINDER

From: Keith Smith
Date: May 23, 2004
Subject: Round One Reminder

My name is Keith Smith and I am conducting tourism security research at Texas A&M University as part of my doctoral studies. You have been nominated by a colleague as a knowledgeable professional in the area of tourism security and suggested that I contact you for your valuable input.

Below you will see the official information sheet approved by the university that describes the research study. The study will be conducted via email for your convenience. It is my desire that the study provide useful information to the tourism industry and the results will be provided to the participants. If you do not wish to participate in the study, an email notification would be appreciated.

It would also be helpful if you could provide the names and contact information of ten other professionals you believe would have knowledge in this area and would provide input.

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

ROUND ONE

SECOND REMINDER

From: Keith Smith
Date: July 9, 2004
Subject: Round One Reminder

I wrote to you a while ago regarding a Ph.D study that I am conducting at Texas A&M University. I would like to involve you in my research. I received your name from a fellow colleague. Please let me know if you would be willing to participate. If you have any questions regarding the study please feel free to me.

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

ROUND ONE

THIRD REMINDER

From: Keith Smith
Date: September 14, 2004
Subject: Round One Reminder

I wrote to you a while ago regarding a Ph.D study that I am conducting at Texas A&M University. I would like to involve you in my research. I received your name from a fellow colleague. Please let me know if you would be willing to participate. If you have any questions regarding the study please feel free to me.

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

ROUND TWO

INVITATION EMAIL

The purpose of this questionnaire is to report all of the ideas sent in response to the first questionnaire and to solicit new ideas for dealing with the issue:

> **What actions can be taken at events and locations frequented by tourists that could reduce the propensity for terror attacks?**

Please further refine these ideas by providing additional clarification where desired and by listing additional strengths and weaknesses you associate with each. Common themes or ideas have been grouped together. Also, rate each idea as to its feasibility and comment as to why the idea is feasible or not. Please list any new ideas at the bottom of the questionnaire and comment on each new idea's strengths and weaknesses for addressing the issue. After receiving all participants' responses to this questionnaire, I will provide you with the results. Then a final questionnaire will be provided in which to assign votes for five ideas you feel will best deal with the issue. All votes will be tallied and results sent to participants. Your ideas will be anonymously included in the next report. For statistical purposes, please provide the number of years of combined experience in Tourism/ Security/ Law Enforcement: _____ yrs.

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

ROUND TWO REMINDER

From: Keith Smith
Date: December 2, 2004
Subject: Round Two Reminder

Thank you so much for participating in my study. I began the process in April and have now received the number of required responses to move into phase 2. I appreciate your efforts and hope to obtain responses from this second request in a timely manner so that we will be able to disseminate the final questionnaire. It is my hopes to wrap up the data collection and provide the results to the participants very quickly, but of course I am dependant upon the responses I receive. Thanks once again and please email me if you have any questions..

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

ROUND THREE

INVITATION EMAIL

The purpose of this study is to elicit your ideas regarding the following issue:

> **What actions can be taken at events and locations (Hotels, Resorts, Theme Parks, Convention Centers, public gatherings, etc.) frequented by tourists that could reduce the propensity for terror attacks?**

The purpose of this final questionnaire is to rank all of the ideas from the previous questionnaires in order of the most critical to the least critical regarding the effect each idea will have against a terror attack. Below is a list of the ideas that were generated in the previous rounds of the study. The list is in no particular order. Please rearrange them in order from top to bottom with regards to your professional opinion as to which idea is the most critical in reducing the propensity of a terror attack. At the bottom of the list should be the idea that in your professional opinion is the least critical action to take in reducing the propensity of a terror attack.

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

ROUND THREE REMINDER

From: Keith Smith
Date: February 1, 2004
Subject: Round Three Reminder

Thank you so much for participating in my study. I began the process in April I appreciate your efforts and hope to obtain responses from this third round in a timely manner so that we will be able to complete the research. It is my hopes to wrap up the data collection and provide the results to the participants very quickly, but of course I am dependant upon the responses I receive. This is the last round and I won't have to ask for any more of your time. I can't tell you how much I appreciate your time.

Thank you very much for your time and participation,

Keith Smith
Research Associate, Texas A&M University
College Station, Texas
Phone: 979-224-3342
Email: TexasAandM.PhDResearch@verizon.net

APPENDIX B

ROUND ONE RESEARCH INSTRUMENT

Round #1

The purpose of this questionnaire is to elicit your ideas regarding the following issue:

> **What actions can be taken at events and locations (Hotels, Resorts, Theme Parks, Convention Centers, public gatherings, etc.) frequented by tourists that could reduce the propensity for terror attacks?**

Please list each idea in a brief, concise manner and email your response to me. Your ideas need not be fully developed. In fact, it is preferable to have each idea expressed in one brief sentence or phrase. Ideas may cover the gamut from hiring practices to implementation of security devices to the amount of cooperation with local law enforcement. No attempt should be made to evaluate or justify these ideas at this point in time. Your ideas will be anonymously included in the next questionnaire.

Idea #1:

Idea #2:

Idea #3:

Idea #4:

Idea #5:

Idea #6:

Idea #7:

Idea #8:

Idea #9:

Idea #10:

APPENDIX C

ROUND TWO RESEARCH INSTRUMENT

Round #2

Idea #1 Terrorism only works due to media. National government needs to have agreements with media regarding a terrorist attack; much the same way they control war footage.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #2 Additional training provided to teach first responders about terrorist goals and their role in limiting the success of a terrorist attack (i.e. what to do after the scene is stabilized).

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #3 Make non-vital targets more readily available in order to channel terrorist activity to those locations. Ensure non-vital targets are politically acceptable.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #4 Publicize as many events as possible being multi-national. Tourism must be advertised for success. Use of in place marketing systems to stress diversity will create additional considerations for terrorist in planning an attack. They don't want the French after them.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #5 Train event and safety specialist in dynamic as opposed to static security techniques. Utilize diverse and randomized methods for screening

tourists upon entry to an event and for controlling crowd flow during an event. Where warranted bag, purse and package checks of guests, participates, invitees and employees; combine assertive measures including inspecting packages, etc but combine those with exceptional customer service empowerment; Bag check stands at entrances to parks and conventions.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #6 In line with dynamic techniques, make heavy use of a double entrance approach. It will be difficult for terrorist to breach if they are unsure what measures will be in place after the initial entrance. Any persons attempting to leave after the first entrance and before the second entrance would be considered suspect; Designing increasing layers of security around an event based upon a risk assessment; Control entrance and egress to and from large events, to include vehicular and pedestrian.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Ideas #7 Improve physical design of facilities to take into account the terrorist threat; DESIGN new facilities with crime prevention in mind; REMODEL existing facilities with crime prevention in mind.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #8 Have a unified method to determine risks.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #9 Reaching out to the community for intelligence. The police have had great success with crime solvers programs and some type of program for voluntary participation in intelligence would be of value.

Establish communication between hotels, parks, and other events with local and federal law enforcement. We have set up an e-mail notification system to distribute flyers and lookouts to the hotels, malls and apartment complexes.

We have for years established a fax system to distribute information to the hotels and theme parks.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #10 Having community leaders speak in a unified voice against terrorism. This would be especially true of community leaders in the religious communities since most recent acts of terrorism are based on some slanted view of religion.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #11 Ask the media's cooperation in correctly portraying these people. They are not suicide bombers but homicide bombers, they are not freedom fighters but murderers, and they are not to be admired but scorned.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #12 Network with other communities to determine what programs have found success in combating this problem.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #13 Implement a crisis management plan.

The first step is to determine what areas of your property or event are vulnerable; evaluate probability and seriousness and then develop a plan to prevent and/or respond if a threat or event occurs.

Conduct threat assessments for special events and structures to include integrated response plans involving private and public first responders.

Start with vulnerability assessments- physical structure and threat assessment- real or perceived

Plan, plan and then review the plan...then plan and evaluate some more. (never feel that you are totally prepared and never feel that you have thought of everything and can not improve on the plan or training).

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #14 Improve intelligence gathering, analysis, and sharing capabilities among private and public security professionals.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #15 Where applicable personal screening of guests, participates, invitees and employees should be conducted.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #16 Back ground checks conducted on each employee; Proper pre-hiring background and credit checks. Not just any background, but PROPER background checks. Ask for more details.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #17 Outside contractors for the event or location should have backgrounds conducted by the contractor.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #18 All employees should have identifying Id's and/or tags.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #19 All working contractors should be provided with a contractor's Id tag or badge.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #20 All employees should come through Security check point and verified that they are an active employee.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #21 All contractors should have a specific parking area and be subject to vehicle screening by Security personnel.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #22 Frequent and high profile public service announcements regarding auspicious activities in or near venue, i.e. citizens should maintain control of their belongings.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #23 Implement the utilization of closed circuit television in tourist areas; Equip venue and core surrounding area with CCTV or microwave surveillance capabilities.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #24 Deployment of plainclothes law enforcement personnel to detect and obtain critical information from within the crowds. Personnel can be used for intelligence gathering and counter surveillance engagement; Deploy special plain-clothes officers to monitor activity at event; have unmarked security guards; Utilization of undercover operatives to gather and disseminate intelligence information both in a strategic and tactical capacity.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #25 Utilization of special units that provide visibility along with confidence to visitors (Examples: Bike patrols, Mounted Units, Motorcycle Units).

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #26 Increase cooperative effort/commitment with federal, state and municipal entities.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #27 Train personnel (both police and private sector) in recognizing potential threats and actions that warrant police intervention.

Provide training to all employees involved in events or tourism venues relating to preoperational surveillance techniques, signs and signatures relating to operational rehearsals, and actions to take when suspicions are raised.

Educate staff using local law enforcement.

TELL your staff to be aware. Don't fall into a comfortable
daze because nothing ever happens.

Training- I have developed a training program for hotels that empowers every employee to be a security agent. Each job category (valet, bell stand, front desk, housekeeping, engineering....) is given things to look for when handling their guests. When something isn't quite right, they contact their security department or call 911 immediately. It gives the employees a sense of involvement in this nations Homeland Security effort.

Train ALL facility employees to recognize and report suspicious activity.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #28 Train, equip and staff police personnel with CBRNE gear.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #29 Target-harden venues to include metal detectors.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #30 Stage specially trained law enforcement personnel for bomb intervention near the venue; Train, staff and deploy personnel in bomb detection/suppression. Deploy mechanical bomb detection devices with police and private sector security staff.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #31 Fund, budget and deploy AIR Unit support to monitor event.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #32 Billboards with directions about what to do if a crisis occurs; SIGN everything; People should always know where they are and where they are going or where they need to go.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #33 Implement the utilization of face recognition software in tourist areas.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #34 High visibility of Security personnel and/or Law Enforcement personnel; Have clothed security guards wandering around; Utilization of High Visibility Uniformed security and/or law enforcement personnel in tourist areas; High visibility of uniformed staff; Heavy police presence in tourism areas keeps most problems away to begin with.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #35 Enhance security procedures to include the use of manual and electronic search methods.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #36 Utilization of Citizen Patrols that have been specifically trained using the Citizen Emergency Response Training model

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #37 PLAN with the local police department.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #38: ASK your guests to be aware. Don't scare them, tell them their stay will be more enjoyable if they are aware of their surroundings and take simple precautions to keep them and their stuff safe.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #39: PARTNER with the media to publish safety tips and location maps.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #40: Available K-9; Use of trained dogs to detect contraband; K9 assistance – bomb dogs.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #41: Regular drills to prevent skill decay; Train and retrain.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #42: Recognize you are a target

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #43: Tighten up loading dock operations at large venues; Only allow access to those on check lists; SOPs for delivery, Any and all delivery vehicles should be recorded and Driver's license should be recorded when making deliveries.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

-

Idea #44: Have regularly scheduled meetings with area venues to keep them up with changing trends in security and to allow them a voice to express their concerns.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #45: Local law enforcement should become involved in organizations and serve on boards when appropriate or when asked to do so. (Hotel and lodging associations, convention and visitors bureaus, chamber of commerce, etc.)

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

Idea #46: Barricades placed to prevent vehicle intrusion; Concrete Barriers and Spike Strips, keep vehicles at a distance from the perimeter; control of vehicular traffic; combat VBIEDs (vehicle-borne improvised explosive device).

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #47 Cross communication with local and fed law enforcement on updated terrorist intelligence.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #48 Off-hour perimeter security (gates, fences, patrols); All outer perimeters should be patrolled on a regular unscheduled time span.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #49 Ongoing training for security personnel on terrorists activity / tactics.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #50 Cameras with a big screen picture of people walking in and around specifically strategic areas of interest – do you see how fast you are driving.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #51 Photo identification, and personalized security devices (cards, bracelets, etc.) for patrons.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

-

Idea #52 Motion detectors that are voice activated and state something to the effect that the premises are under law enforcement surveillance.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #53 Advanced reservations required to access vital places. Scan cards were mailed to allow access to the event.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

-

Idea #54 Use radioactive material detection devices throughout facilities or event areas.

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to	Not Feasible	Feasible	Easily

be Implemented			accomplished

What are the barriers to implementing the solution:

-

New Idea:

• Your clarification (if any):

• Strengths:

• Weaknesses:

• Feasibility:

1	2	3	4
Not Likely to be Implemented	Not Feasible	Feasible	Easily accomplished

What are the barriers to implementing the solution:

APPENDIX D

ROUND THREE RESEARCH INSTRUMENT

ROUND #3

The purpose of this final questionnaire is to rank all of the ideas from the previous questionnaires in order of the most critical to the least critical regarding the effect each idea will have against a terror attack. Below is a list of the ideas that were generated in the previous rounds of the study. The list is in no particular order. Please rearrange them in order from top to bottom with regards to your professional opinion as to which idea is the most critical in reducing the propensity of a terror attack. At the bottom of the list should be the idea that in your professional opinion is the least critical action to take in reducing the propensity of a terror attack.

- All working contractors should be provided with a contractor's Id tag or badge.
- All employees should come through security check point and verified that they are an active employee.
- Improve physical design of facilities to take into account the terrorist threat. Design new facilities with crime prevention in mind. Remodel existing facilities with crime prevention in mind.
- Have a unified method to determine risks.
- Reach out to the community for intelligence. Establish communication between hotels, parks, and other events with local and federal law enforcement.
- Network with other communities to determine what programs have bee successful in combating terrorism.
- Terrorism only works due to media. National government needs to have agreements with media regarding a terrorist attack; much the same way they control war footage.
- Additional training provided to teach first responders about terrorist goals and their role in limiting the success of a terrorist attack (i.e. what to do after the scene is stabilized).
- Make non-vital targets more readily available in order to channel terrorist activity to those locations. Ensure non-vital targets are politically acceptable.
- Implement a crisis management plan. Conduct threat assessments for special events and structures to include integrated response plans involving private and public first responders.

- Improve intelligence gathering, analysis, and sharing capabilities among private and public security professionals.
- Where applicable, personal screening of guests, participates, invitees, and employees should be conducted.
- Conduct thorough background and credit checks on each employee.
- Outside contractors for the event or location should have backgrounds conducted on own employees by third party.
- All employees should have identifying badges and/or tags.
- All contractors should have a specific parking area and be subject to vehicle screening by security personnel.
- Frequent and high profile public service announcements regarding suspicious activities in or near venue, i.e. patrons should maintain control of their belongings.
- Deploy plainclothes law enforcement personnel to detect and obtain critical information from within the crowds. Personnel can be used for intelligence gathering and counter surveillance engagement.
- Utilize special security units that provide confidence to visitors (Examples: Bike patrols, Mounted Units, Motorcycle Units).
- Having community leaders, including religious leaders, speak out in a unified voice against terrorism since most recent acts of terrorism are based on some slanted view of religion.
- Ask the media's cooperation in correctly portraying these people. They are not suicide bombers, but homicide bombers, they are not freedom fighters, but murderers, and they are not to be admired, but scorned.
- Increase cooperative effort/ commitment with federal, state and municipal entities.
- Implement the utilization of closed circuit television in tourist areas at venue and core surrounding area.

- Design increasing layers of security around an event based upon a risk assessment. In line with dynamic techniques, make heavy use of a double entrance approach; it will be difficult for terrorists to breach if they are unsure what measures will be in place after the initial entrance. Any persons attempting to leave after the first entrance and before the second entrance would be considered suspect.
- Train, equip, and staff police personnel with CBRNE gear.
- Target-harden venues to include metal detectors.
- Utilize off-hour perimeter security patrols at gates and fences. All outer perimeters should be patrolled on a regular unscheduled time span.
- Stage specially trained law enforcement personnel for bomb intervention near the venue. Train staff and deploy personnel in bomb detection/suppression. Deploy mechanical bomb detection devices with police and private sector security staff.
- Employ cameras with a big screen picture of people walking in and around specific strategic areas of interest. Similar to radar trailers; “Do you see how fast you are driving?”
- Fund, budget, and deploy air unit support to monitor event.
- Billboards with instructions on what to do if a crisis occurs. People should always know where they are and where they are going or where they need to go.
- Implement the utilization of face recognition software in tourist areas.
- High visibility of law enforcement personnel for a deterrent aspect.
- Enhance security procedures to include the use of manual and electronic search methods.
- Utilize citizen patrols that have been specifically trained to enhance security or law enforcement.
- Plan with the local police department.
- Provide ongoing training for security personnel on terrorists’ activity and tactics.

- Use photo identification and personalized security devices (i.e. ID cards, bracelets, etc.) for patrons.
- Install motion detectors that are voice activated and state something to the effect that the premise is under law enforcement surveillance.
- Ask your guests to be aware. Don't scare them. Tell them their stay will be more enjoyable if they are aware of their surroundings and take simple precautions to keep them and their belongings safe.
- Partner with the media to publish safety tips and location maps.
- Use training drills to prevent skill decay. Train and retrain.
- Recognize you (tourism venue) are a target.
- Tighten-up security at loading dock operations at large venues. Only allow access to those on check lists. Implement standard operating procedures for delivery. Any and all delivery vehicles should be recorded and driver's license should be recorded.
- Have regularly scheduled meetings with area venues to keep them informed of changing trends in security and to allow them a voice to express their concerns.
- Local law enforcement should become involved in organizations and serve on boards when appropriate or when asked to do so; i.e. hotel and lodging associations, convention and visitors bureaus, chamber of commerce, etc.
- Use barricades to prevent vehicular intrusion. Employ concrete barriers and spike strips. Keep vehicles at a distance from the perimeter.
- Cross communicate with local and fed law enforcement on updated terrorist intelligence.
- Use of trained dogs to detect weapons/ contraband. Deploy K9 units to assist in bomb detection.
- Use radioactive material detection devices throughout facilities or event areas.
- Require advanced reservations to access vital places. Scan cards are mailed to allow access to the event.

VITA

Clifford Keith Smith
1108 Dominik
College Station, Texas 77840

Education

Ph.D., Educational Human Resource Development Texas A&M University, College Station, Texas (2006).

M.S., Educational Human Resource Development; Texas A&M University, College Station, Texas (1997).

B.S., Industrial Education; Texas A&M University, College Station, Texas (1989).

Professional Experience

Eighteen years as a police officer serving in the capacity of Patrol Officer, Narcotics Investigator, Patrol Watch Commander, Special Services Division Commander, Accreditation Compliance Commander, Assistant SWAT Commander, The City of College Station.

Six years simultaneously with above as Adjunct Staff Instructor, Texas A&M University Riverside Campus, Law Enforcement Training Division.

Three years simultaneously with above as Adjunct Staff Instructor, Texas Association of Counties.

Instructor Presentation and Training Development

Have trained over eighty separate law enforcement agencies in the areas of Tactical Operations, Undercover Operations, Critical Incident Command, Policy Writing, Training Division Development, and First Line Supervisor.

Published Article

Smith, C.K. (2001). Responsibility for Training Topic Selection. *Command, the Journal of the Texas Tactical Police Officers Association*, Spring 2001.